ISTITUTO COMPRENSIVO GIOSUÈ CARDUCCI
P.zza Sforzini, 18 – 57128 Livorno Tel. 0586/502356
CF: 92144980494 codice univoco: 5I1ZGB
www.scuolecarducci.livorno.it www.scuolecarduccilivorno.edu.it
LIIC82200P@ISTRUZIONE.IT LIIC82200P@PEC.ISTRUZIONE.IT

DOCUMENTO DI ePOLICY

I.C. "GIOSUE' CARDUCCI" LIIC82200P

PIAZZA ALFREDO SFORZINI, 18
57128 LIVORNO (LI)

INDICE

CAPITOLO 1 - SCOPO DELL'ePOLICY

Il presente documento ha lo scopo di promuovere l'uso consapevole e critico delle tecnologie digitali e di Internet, ossia le regole per un uso corretto e responsabile degli strumenti tecnologici collegati alla rete; accogliendo come normativa di riferimento le indicazioni di Educazione Civica Digitale emanate dal Ministero dell'Istruzione, per salvaguardare e proteggere gli studenti e tutto il personale dell'istituzione scolastica didattica.

L'Istituto Comprensivo G. Carducci intende promuovere lo sviluppo della competenza digitale attraverso la conoscenza di procedure e competenze tecniche e di norme comportamentali, dettate da un uso consapevole e critico da parte degli studenti e studentesse, delle tecnologie digitali e della rete Internet. Lo scopo è, dunque, prevenire e eventualmente rilevare e affrontare situazioni derivanti da un uso pericoloso delle stesse. Il nostro obiettivo passa attraverso una campagna di promozione delle competenze di cittadinanza digitale, sensibilizzando docenti, studenti, alunni e famiglie relativamente all'uso consapevole di Internet e delle tecnologie digitali. I/le docenti hanno il compito di responsabilizzare i/le discenti nell'uso consapevole e responsabile delle apparecchiature della scuola, che sono patrimonio comune, e nel seguire le corrette norme di utilizzo. Per garantire la sicurezza in rete la scuola ha previsto le seguenti strategie:

- informare alunni e alunne dei rischi cui si espongono nella navigazione in rete;
- promuovere la partecipazione del personale docente a corsi di formazione sull'uso delle TIC nella didattica e sull'uso consapevole di Internet;
- orientarsi verso una didattica digitale educativa, indirizzandosi verso il Coding e il pensiero computazionale;
- accesso guidato ai computer scolastici;
- condividere materiali (guide, manuali, ecc..) sull'uso consapevole di Internet e delle tecnologie digitali.

1.1 PRESENTAZIONE DELL'ePOLICY

Attraverso l'ePolicy il nostro Istituto vuole dotarsi di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.
L'ePolicy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che sensibilizzare ad un uso consapevole delle stesse.
Finalità del presente documento è regolamentare in modo organico e condiviso dall'intera Comunità Scolastica i comportamenti e le procedure in merito all'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) nella didattica, promuoverne un uso critico e consapevole, prevenire, rilevare, gestire e contrastare le problematiche derivanti da un uso ignaro ed improprio delle tecnologie digitali. Il nostro Istituto riconosce come le TIC rappresentino una grande opportunità per sostenere l'insegnamento, promuovere la creatività, stimolare la consapevolezza e migliorare l'apprendimento degli studenti, ma è conscio dei rischi relativi e della conseguente necessità di fronteggiarli adeguatamente.

Con questa ePolicy si è deciso di adottare una politica di prevenzione attraverso:

- La messa in campo di azioni informative e di confronto volte al riconoscimento precoce di comportamenti a rischio con lo scopo di intervenire prima della possibile insorgenza di fenomeni veri e propri di bullismo e /o cyberbullismo, azioni che possano promuovere l'uso consapevole e funzionale delle tecnologie e dei social.
- La promozione di interventi educativi e azioni a supporto di studenti e studentesse vittime di cyberbullismo o di problematiche relative all'utilizzo della rete, in linea con la legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo".
- La realizzazione di progetti d'Istituto che siano caratterizzati da multidisciplinarietà con il coinvolgimento e il supporto di figure esterne qualificate (es. educatori, psicologi, esperti informatici, polizia postale, ecc.).

1.2 RUOLI E RESPONSABILITA'

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, si impegni nell'attuazione e promozione di essa.

Ogni utente appartenente alla comunità educante nel momento in cui utilizza la rete deve:

- rispettare il presente documento e la normativa vigente;
- tutelare la privacy di tutti gli utenti coinvolti;
- rispettare la "netiquette" ed il galateo della rete.

All'interno della comunità educante ogni figura ha un ruolo specifico:

La Dirigente Scolastica promuove l'uso consapevole delle tecnologie e di Internet garantendo la sicurezza, anche online, di tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento e le indicazioni del Ministero dell'Istruzione. Inoltre, avvalendosi del team per la prevenzione delle bullismo/cyber bullismo sollecita la partecipazione a corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. In caso di episodi manifesti di bullismo e/o cyberbullismo ed uso improprio delle tecnologie digitali ha il compito di intervenire sia sul piano educativo sia attraverso sanzioni.

DS con DSGA (GESTORI DATI E INFORMAZIONI)

- Assicurare nei limiti delle risorse finanziarie disponibili l'intervento di tecnici per garantire che l'infrastruttura tecnologica della scuola sia funzionante, sicura, non aperta ad uso improprio o a dannosi attacchi esterni;
- favorire il funzionamento dei diversi canali di comunicazione all'interno della scuola e fra la scuola e le famiglie;
- garantire che i dati di gestione siano accurati e aggiornati;
- promuovere le migliori pratiche nella gestione delle informazioni, ossia mettere in atto un sistema di controllo di accesso appropriato. I dati sono utilizzati, trasferiti e cancellati in linea con i requisiti di protezione dei dati;
- mantenere i controlli di accesso per proteggere le informazioni sensibili archiviate

su dispositivi di proprietà della scuola.

L'Animatrice digitale ha il compito di promuovere corsi di formazione d'Istituto sulle TIC, supportare il personale scolastico sia dal punto di vista tecnico e informatico sia in merito alla tutela della privacy e, inoltre, può monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola controllando che tutti gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Il Referente bullismo e cyberbullismo "Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo"[1]. Tale docente ha il compito di coordinare e promuovere azioni specifiche per la prevenzione e il contrasto del fenomeno del bullismo e del cyberbullismo. Sono state nominate sei referenti, una per ogni plesso di scuola primaria e secondaria di 1° grado. La scuola può avvalersi della collaborazione delle Istituzioni, delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Il team prevenzione bullismo e cyberbullismo può coinvolgere in progetti e percorsi formativi tutta la comunità educante.

I/Le Docenti hanno un ruolo molto importante poiché hanno il compito di diffondere la cultura dell'uso responsabile e consapevole delle TIC e della Rete. Possono utilizzare le TIC nella didattica della propria disciplina per offrire più strumenti a studenti e studentesse, a alunni e alunne. I/le docenti devono supportare alunni e alunni, studenti e studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici connessi in Rete. Inoltre, hanno il compito di educarli all'importanza del rispetto della privacy. È importante che tutti siano informati sui rischi presenti in Rete, vanno educati ad un uso consapevole in modo che Internet possa essere una fonte di divertimento oltre che un utile strumento di apprendimento. I docenti devono osservare i comportamenti a rischio e hanno il dovere morale e professionale di segnalare alla Dirigente Scolastica, la quale insieme ai n.6 Referenti per il Bullismo e Cyberbullismo e al Consiglio di Classe potrà definire strategie di intervento condivise. Tutti i docenti devono impegnarsi a garantire la riservatezza dei dati personali, trattati ai sensi della normativa vigente, controllare l'accesso a Internet e l'uso delle tecnologie digitali e dei dispositivi mobili da parte degli alunni, durante le attività scolastiche (ove previsto e consentito), devono inoltre segnalare alla DS qualsiasi difficoltà.

Personale ATA deve essere coinvolto nell'applicazione della legge 107/2015[2] che concerne non solo il tempo scuola e il potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA è coinvolto nelle pratiche di prevenzione perché è tenuto alla segnalazione di comportamenti non adeguati e/o agli episodi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse, gli Alunni e le Alunne devono dimostrare di saper utilizzare in modo consapevole le tecnologie digitali in coerenza con quanto richiesto dai do-

[1] Art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo",
[2] "La Buona Scuola"

centi. Con il supporto della scuola devono partecipare ai progetti e alle attività proposte sull'utilizzo consapevole delle TIC. Adottare comportamenti rispettosi degli altri anche nella comunicazione in rete, comunicare difficoltà e bisogni nell'utilizzo delle tecnologie digitali ai docenti e ai genitori.

I Genitori hanno il compito di collaborare 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 dei device personali. Come parte della comunità educante, sono tenuti a relazionarsi con i docenti sulle linee educative che riguardano le TIC e la Rete e hanno il dovere di confrontarsi con loro nel momento in cui rilevano che i propri figli fanno un uso scorretto e poco responsabile delle tecnologie digitali o di Internet. È importante che accettino e condividano quanto scritto nell'ePolicy dell'Istituto e nel patto di corresponsabilità, in un'ottica di collaborazione reciproca.

1.3 CONDIVISIONE E COMUNICAZIONE DELL'ePOLICY ALL'INTERA COMUNI-TÀ SCOLASTICA

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

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

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

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto. Il documento ePolicy verrà pubblicato sul sito della scuola e condiviso con tutta la comunità educante. Tutti gli studenti e le studentesse saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno utilizzati solo con l'autorizzazione degli insegnanti. Gli alunni e le alunne verranno educati all'uso responsabile e sicuro di Internet.

Il documento sarà discusso e condiviso negli organi collegiali e successivamente sarà condiviso con i genitori. Per tutto il personale sono previsti aggiornamenti e nuova formazione in materia di sicurezza online.

CAPITOLO 2 - FORMAZIONE E CURRICOLO

2.1 CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

Gli studenti e le studentesse usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (in-

clusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico"[3].
Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e l'implementazione di un curricolo digitale.

La competenza digitale, per la sua importanza nelle attività professionali e anche quotidiane, è ritenuta dall'Unione Europea una competenza chiave per lo sviluppo del senso di cittadinanza. Nel curricolo disciplinare del nostro Istituto tale competenza pervade in modo trasversale i vari insegnamenti; questa declinazione scaturisce dalla necessità di iniziare a dare una formazione di base sull'uso delle TIC, inserendole nelle attività didattiche, per arrivare nelle classi finali a fornire gli strumenti per un approccio consapevole, critico, autonomo e responsabile. Il curricolo scolastico degli studenti viene integrato con attività educative che favoriscono la cultura della sicurezza on line. In tal senso si impegna a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni e delle alunne e direttamente proporzionali ad essa, tra cui:

- programmare attività e far partecipare gli alunni a laboratori di Coding;
- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza, sviluppando il pensiero critico;
- assumere comportamenti adeguati in ambienti on line, rispettosi della dignità propria e altrui;
- essere consapevoli che dati personali e fotografie possono essere manipolate e usate in maniera fraudolenta e lesiva da parte di terzi;
- comprendere che le "identità virtuali" possono essere ingannatorie;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- conoscere le norme in materia di copyright;
- sviluppare una sempre maggiore sensibilità verso l'impatto che il cyberbullismo e altri comportamenti scorretti possono avere sulla vita propria, dei compagni e delle compagne e sapere a chi rivolgersi per segnalare eventuali difficoltà.

2.2 FORMAZIONE DEI DOCENTI SULL'UTILIZZO E L'INTEGRAZIONE DELLE TIC (TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE) NELLA DIDATTICA

È fondamentale che tutti i docenti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo. Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.
In attuazione del PNSD questo Istituto ha realizzato:

[3] ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).

- individuazione e formazione dell'Animatrice Digitale coadiuvata dal team digitale;
- formazione dei docenti all'utilizzo del registro elettronico e dello scrutinio elettronico;
- somministrazione di un questionario rivolto ai docenti per la rivelazione dei bisogni "digitali";
- ricognizione e messa a punto delle dotazioni digitali;
- attivazione e comunicazione di iniziative di formazione rivolte allo sviluppo e alla diffusione del Coding e del pensiero computazionale.

2.3 SENSIBILIZZAZIONE DELLE FAMIGLIE E INTEGRAZIONI AL PATTO DI CORRESPONSABILITA'

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

L'Istituto ha promosso e continua a promuovere iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti incontri fra studenti/studentesse e specialisti (docenti, forze dell'ordine) per la diffusione del materiale informativo su queste tematiche. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Sul sito scolastico saranno messi in condivisione materiali dedicati ad alunni e alle famiglie come guide in formato pdf, link e video che possono fornire spunti di approfondimento e confronto. La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (ePolicy), per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto, e prevenire i rischi legati a un utilizzo non corretto di Internet. L'istituto intrattiene rapporti costanti e sistematici con le famiglie e le informa, tramite il registro elettronico, delle attività proposte a genitori e studenti. Comunica l'andamento didattico - disciplinare dei singoli alunni e delle singole alunne tramite il coordinatore di classe. In questo senso, la Scuola ha elaborato il Patto Educativo di Corresponsabilità che rappresenta un'alleanza educativa ove sono definiti in maniera dettagliata e condivisa i diritti e i doveri presenti nel rapporto tra Istituzione scolastica autonoma, studenti e famiglie. Con la sottoscrizione del Patto Educativo i firmatari

si assumono precise responsabilità anche in conformità con la normativa vigente.

CAPITOLO 3 - GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA.

3.1 PROTEZIONE DEI DATI PERSONALI

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta tali dati possono riguardare informazioni sensibili. Il "corretto trattamento dei dati personali" a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.
La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).
Anche le scuole, quindi, hanno l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.
Il trattamento dei dati personali, ai sensi e per l'effetto della legge 31/12/1996 n. 675 e del GDPR Regolamento UE 2016/679, è uniformato ai principi del rispetto dei diritti, delle libertà fondamentali e della dignità delle persone con particolare riferimento alla riservatezza e all'identità personale. L'impegno sarà rivolto a non diffondere i dati personali in possesso della scuola, siano essi relativi agli studenti/studentesse, al personale, ad enti esterni, se non per gli obblighi di legge.
I/Le docenti dell'Istituto sono nominati dalla Dirigente scolastica quali incaricati del trattamento dei dati personali degli alunni e delle loro famiglie, ai fini dello svolgimento delle proprie funzioni istituzionali e nel rispetto della normativa vigente.

3.2 ACCESSO A INTERNET

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche*

oltre che da situazioni di vulnerabilità personale e disabilità.

Il diritto di accesso a Internet è presente nell'ordinamento italiano ed europeo[4] e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti e studentesse che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet "diventi una realtà, a partire dalla scuola".

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

Si progetta con la collaborazione dell'assistenza tecnica specializzata un piano di revisione del sistema di filtraggio presente nei vari plessi, così da evitare il più possibile l'accesso a siti inappropriati al contesto scolastico. Per quanto riguarda l'utilizzo di software antivirus si opta per l'utilizzo di programmi gratuiti, scegliendo quelli considerati dal personale tecnico più efficaci. Ai tecnici si affida il compito di mantenere costantemente aggiornati i suddetti software. Tutti coloro che utilizzano i supporti multimediali della scuola saranno sensibilizzati ad eseguire una scansione antivirus quando collegano dispositivi personali di archiviazione esterna. Tutti i plessi dell'Istituto sono dotati di una rete wireless alla quale sono connessi la maggior parte dei dispositivi; ove possibile e conveniente (per es. laboratori di informatica) si procede alla connessione alla rete Internet attraverso cavo.

I dispositivi sono collegabili alla rete Internet esclusivamente tramite password. Si ritiene utile che il personale docente di ogni plesso, la docente Responsabile di plesso o la componente del Team digitale di plesso, sia a conoscenza della password di accesso, così da poter connettere facilmente tutti i dispositivi necessari per lo svolgimento delle attività didattiche.

3.3 STRUMENTI DI COMUNICAZIONE ONLINE

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

Il personale interno alla scuola (DS, docenti, personale di segreteria) e i genitori hanno a disposizione il Portale Argo per il registro elettronico "Argo Didup" e per le comunicazioni interne. L' Istituto utilizza Google Workspace for Education Fundamentals protetto da un

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

cloud appositamente creato per la scuola che rispetta tutte le norme e le indicazioni del GDPR. Il sistema permette la creazione di account individuali utilizzabili anche da utenti che non abbiano compiuto l'età legale prevista per l'utilizzo di strumenti cloud. Ogni alunno e ogni personale della scuola (Dirigente, docenti, personale ATA) dispongono del proprio account istituzionale con le conseguenti responsabilità che sono collegate ad esso.
L'Istituto Carducci dispone di appositi strumenti di comunicazione come:

- Indirizzo di posta elettronica personale di istituto: cognome.nome@scuolacarducci.com cognome.nome@scuolecarduccilivorno.edu.it
- mailing list di gruppo: (CDC, plesso, interplesso ecc.)
- Studenti, docenti e genitori sono informati sul fatto che **non** è consentito l'utilizzo di strumenti non autorizzati (es. Whatsapp, Instagram, Facebook, messaggistica privata).
- Meet: lo strumento per effettuare videoconferenze.
- Il registro elettronico "Argo Didup" permette il necessario adempimento amministrativo di rilevazione della presenza in servizio dei docenti e la registrazione della presenza degli alunni e delle alunne a lezione, così come per le comunicazioni scuola-famiglia e l'annotazione delle attività giornaliere e dei compiti. Inoltre, è uno strumento che consente la comunicazione tra la scuola e le famiglie. Questa piattaforma permette ai genitori di visualizzare e giustificare le assenze del proprio figlio, utilizzare la bacheca elettronica , le circolari, l'argomento delle lezioni, i risultati degli scrutini.
- Sito web della scuola: (https://www.scuolecarduccilivorno.edu.it/) è la prima e principale interfaccia dell'Istituto. Oltre alle informazioni generali e di contatto, vi si trovano apposite sezioni dedicate alle Scuole, ai Servizi, alla Didattica, ai Progetti nonché fondamentali comunicazioni, informazioni, modulistica per docenti, personale ATA alunni e famiglie.

3.4 STRUMENTAZIONE PERSONALE

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/delle studenti/esse e del personale docente ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il PNSD.
La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Ministero dell'Istruzione per l'uso dei dispositivi mobili a scuola, BYOD, "Bring your own device"[5].
Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.
La tecnologia, se utilizzata in modo responsabile e corretto, fornisce agli studenti e alle studentesse, opportunità innovative per incrementare la loro cultura, in linea con quanto specificato nel PNSD. Il nostro Istituto vuole favorire tale processo garantendone la sicu-

[5] https://scuoladigitale.istruzione.it/pnsd/ambiti/ambienti-e-strumenti/azione-6-linee-guida-per-politiche-attive-di-byod-bring-your-own-device/

rezza attraverso una modalità di interazione che contribuisca al miglioramento dell'ambiente educativo e di apprendimento. Pertanto, l'uso improprio dei dispositivi digitali mobili a scuola non è ammesso e viene sanzionato, in relazione alla gravità dell'infrazione, in base a quanto stabilito dal Regolamento di Istituto.
Sono ammessi a scuola i dispositivi come computer portatile, tablet, e-reader; non sono ammessi cellulari, smartphone, videogiochi in genere.
I dispositivi devono essere usati a scuola per soli scopi didattici e solo con l'autorizzazione dell'insegnante. Agli studenti non è permesso usare dispositivi elettronici per giochi durante le ore scolastiche.
È vietato agli studenti usare dispositivi di registrazione audio, videocamere o fotocamere per registrare video o fare foto in classe senza il permesso dell'insegnante. E' previsto l'utilizzo di questi dispostivi solo previa richiesta presentata dall'insegnante alla DS.

CAPITOLO 4 - RISCHI ON LINE: CONOSCERE, PREVENIRE E RILEVARE

4.1 SENSIBILIZZAZIONE E PREVENZIONE

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

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

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

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

Il nostro Istituto promuove l'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali, con l'obiettivo di ridurre le situazioni di rischio attraverso azioni che coinvolgono:

I docenti:

- attraverso la formazione personale dei docenti grazie a specifici corsi di aggiornamento offerti dallo stesso Istituto o da Enti qualificati;

- attraverso l'adesione a progetti dedicati: progetti d'istituto, attività proposte da enti qualificati.

Gli alunni:

- attraverso l'inserimento di ore di educazione alla cittadinanza digitale all'interno del curricolo di Educazione Civica;
- attraverso l'organizzazione di incontri formativi e di attività con i docenti e gli esperti per affrontare i rischi on line;
- attraverso l'adesione a progetti dedicati.

I Genitori:

- proponendo loro di aderire a progetti specifici con incontri di consulenza da parte di esperti;
- attraverso l'adeguamento del Regolamento d'Istituto e del Patto di Corresponsabilità;
- attraverso colloqui costanti con i docenti del consiglio di classe.

4.2 CYBERBULLISMO: CHE COS'È E COME PREVENIRLO

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

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

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.

Nomina delle Referenti per le iniziative di prevenzione e contrasto con il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, possono richiedere la collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

Gli atti di cyberbullismo possono essere raggruppati in due grandi gruppi:

- **cyberbullismo diretto:** si verifica quando il bullo utilizza strumenti di messaggistica

istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei, come ad esempio nei casi di:

- ✓ Flaming: litigi online nei quali si fa uso di un linguaggio violento e volgare;
- ✓ Harassment: molestie attuate attraverso l'invio ripetuto di linguaggi offensivi;
- ✓ Cyberstalking: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità.

• **cyberbullismo indiretto**: si verifica quando il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico. A titolo esemplificativo si possono ricordare:

- ✓ Denigrazione: pubblicazione all'interno di comunità virtuali, quali newsgroup, blog, forum di discussione, messaggistica immediata, siti Internet, di pettegolezzi e commenti crudeli, calunniosi e denigratori;
- ✓ Outing estorto: registrazione delle confidenze, raccolte all'interno di un ambiente privato, creando un clima di fiducia e poi inserite integralmente in un blog pubblico;
- ✓ Impersonificazione: insinuazione all'interno dell'account di un'altra persona con l'obiettivo di inviare dal medesimo messaggio ingiurioso che screditino la vittima.

È inoltre importante ricordare che diventa cyberbullismo anche **l'esclusione**, quando assume una forma di estromissione intenzionale e ripetuta di un individuo dall'attività online. I ragazzi e le ragazze che fanno azioni di bullismo possono commettere reati.
Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

- percosse (art. 581);
- lesione personale (art. 582);
- ingiuria (art. 594);
- diffamazione (art. 595);
- violenza privata (art. 610);
- minaccia (art. 612);
- danneggiamento (art. 635).

Negli atti di bullismo/cyberbullismo vanno distinte le diverse responsabilità ed a tal riguardo si identificano:

1. Culpa del minore

Occorre fare una distinzione tra il minore di 14 anni e quello con un'età compresa tra i 14 ed i 18 anni. Il minore di 14 anni non è mai imputabile penalmente. Se viene però riconosciuto come "socialmente pericoloso" possono essere previste misure di sicurezza. Il minore tra i 14 e i 18 anni di età è imputabile se viene dimostrata la sua capacità di intendere e volere. La competenza a determinare la capacità del minore è del giudice che si avvale di consulenti professionali.

2. Culpa in vigilando ed educando dei genitori

Si applica l'articolo 2048 del codice civile. Il non esercitare una vigilanza adeguata all'età e indirizzata a correggere comportamenti inadeguati (culpa in educando e vigilando) è alla base della responsabilità civile dei genitori per gli atti illeciti commessi dal figlio minorenne

che sia capace di intendere e di volere. A meno che i genitori del minore non dimostrino di non aver potuto impedire il fatto, sono oggettivamente responsabili.

3. Culpa in vigilando e in organizzando della Scuola

L'art.28 della Costituzione Italiana recita che "I funzionari ed i dipendenti dello Stato e degli Enti pubblici sono direttamente responsabili, secondo le leggi penali, civili ed amministrative, degli atti compiuti in violazioni di diritti. In tali casi la responsabilità si estende allo Stato ed agli altri enti pubblici." Dal punto di vista civilistico trova, altresì, applicazione quanto previsto all'Art. 2048 del codice civile, secondo comma, che stabilisce che "i precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi e apprendisti nel tempo in cui sono sotto la loro vigilanza". La presunzione di colpa può essere superata solamente laddove si dimostri di aver adeguatamente vigilato ovvero si dia la prova del caso fortuito. Per superare la presunzione, la scuola deve dimostrare di adottare "misure preventive" atte a scongiurare situazioni antigiuridiche.

Al fine di prevenire il fenomeno del cyberbullismo il nostro Istituto ha:

- individuato i referenti di ogni plesso scuola primaria e secondaria di 1° grado per la prevenzione e il contrasto del bullismo e del cyberbullismo;
- formato un TEAM di lavoro;
- stimolato un ruolo attivo degli studenti/alunni in attività di peer education, cooperative learning e circle time;
- stabilito le procedure di intervento in caso di atti di bullismo/cyber bullismo;
- previsto l'attivazione di uno sportello di ascolto e di aiuto offerto dal referente di plesso;
- fissato azioni preventive ed educative e non solo sanzionatorie.

Gli interventi preventivi ed educativi includono:

- la diffusione e condivisione con gli alunni e le loro famiglie delle iniziative che l'Istituto ha intrapreso, come quelle elencate nel paragrafo precedente;
- l'attuazione di progetti, con l'eventuale contributo esterno di figure professionali, per ampliare le conoscenze digitali degli alunni, creando in loro la consapevolezza dei rischi connessi all'utilizzo della rete;
- i progetti che mirano all'Inclusione, alla valorizzazione delle differenze e valorizzano la gentilezza come forma principale di comunicazione tra pari;
- la formazione ad un uso corretto degli strumenti informatici e l'organizzazione e le regole di utilizzo delle aule di informatica.

Le misure non solo sanzionatorie prevedono:

- attività di natura sociale/culturale che vadano a vantaggio della comunità scolastica: es. svolgimento di azioni positive, quali lettera di scuse a vittima e famiglia, pulizia dei locali, attività di ricerca, riordino materiali, produzione di lavori scritti/artistici che inducano lo studente a riflettere e rielaborare criticamente gli episodi accaduti;
- sospensione attiva a scuola, con svolgimento di attività rieducative.

4.3 FORME DI CYBERBULLISMO
HATE SPEECH: CHE COS'È E COME PREVENIRLO

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo. Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante è affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di coscienza consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni da intraprendere in relazione a questa problematica.
Il nostro Istituto propone specifiche attività didattiche per fornire agli studenti gli strumenti necessari per contrastare e destrutturare gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati all'etnia, al genere, all'orientamento sessuale, alla disabilità. Inoltre, promuove la partecipazione civica e sensibilizza i/le ragazzi/e i/le bambini/e ad utilizzare **il linguaggio della gentilezza**.

Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete. L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale.
È ormai diffusa la consapevolezza del ruolo che la tecnologia gioca nella quotidianità dei nostri studenti e delle nostre studentesse e dell'impatto che ha sulla qualità della loro vita. Gli elementi che contribuiscono al benessere digitale che possono essere oggetto di riflessione a scuola sono:

- la ricerca di equilibrio nelle relazioni anche online,
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali,
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile,
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

Da questo punto di vista la didattica può far emergere il potenziale delle nuove tecnologie anche con attività specifiche che facciano emergere la funzionalità dei dispositivi e che al tempo stesso aiutino a prendere consapevolezza rispetto al rischio della dipendenza da Internet.

Sexting

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

Il nostro Istituto intende proporre percorsi di educazione all'affettività e alla sessualità al fine di rendere le alunne e gli alunni più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro. I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di teen dating (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

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

A seguire vengono descritte le azioni da intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

- Promuove la formazione sui rischi dell'adescamento on line durante gli incontri specifici con esperti (forze dell'ordine, polizia postale, psicologa …) rivolti agli studenti, ai genitori e agli insegnanti sul tema della Web reputation e dell'uso improprio delle nuove tecnologie.

I casi di adescamento online richiedono l'intervento delle Forze dell'Ordine.

Pedopornografia

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

La legge n. 269 del 3 agosto 1998 "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle

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

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

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

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

Qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, alle forze dell'ordine o alle varie Hot line dedicate.

Il nostro Istituto affronta il tema della pedopornografia legata al fenomeno del sexting durante gli incontri con esperti (forze dell'ordine, polizia postale, psicologa …) sui rischi dell'uso improprio delle nuove tecnologie.

Casi di pedopornografia richiedono l'intervento delle Forze dell'Ordine.

CAPITOLO 5 - SEGNALAZIONE E GESTIONE DEI CASI

5.1 COSA SEGNALARE

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

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse, alunne e alunni (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.

Nelle procedure:

- sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso;

- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre alla Dirigente Scolastica.

Inoltre, la scuola individua le figure che costituiranno un team preposto alla gestione della segnalazione.
Nell'affrontare i casi prevediamo la collaborazione con 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.
Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

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

- **Cyberbullismo**
- **Adescamento online**
- **Sexting**

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore e 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.**

I docenti seguono le procedure standardizzate, presenti in allegato, per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse.
Nel caso in cui si ipotizzi che ci si possa trovare di fronte ad una fattispecie di reato come ad esempio, il furto di identità o la persistenza di una condotta persecutoria che mette seriamente a rischio il benessere psicofisico del bambino/a o dell'adolescente coinvolto/a in qualità di vittima si farà riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione.

5.2 COME SEGNALARE: QUALI STRUMENTI E A CHI

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.
Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere

sempre gestite anche a livello di gruppo.
Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyber-bullismo, sexting o adescamento online.
- CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyber-bullismo, sexting o adescamento online.

Per tutti i dettagli fare riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti e studentesse

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**:

- 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.
- studenti e studentesse possono rivolgersi alle Helpline dedicate.

E' opportuno precisare le procedure previste nei due casi sopraccitati.

Nel CASO A, il/la docente deve:

avvisare il Coordinatore/la Coordinatrice ed eventualmente l'intero consiglio di classe, coinvolgere il Referente di plesso per il contrasto del bullismo e del cyberbullismo valutando insieme le possibili strategie d'intervento, se si ravvisa la necessità e l'urgenza coinvolgere la Dirigente Scolastica.

Nel frattempo, il/la docente (in collaborazione con i docenti informati) ascolta gli studenti e le studentesse, osservando e monitorando il clima di classe, ciò che accade, le dinamiche relazionali nel contesto classe, senza fare indagini dirette. Se non si configura un caso di bullismo, è comunque opportuno riflettere sul clima della classe e sulla qualità delle relazioni. Tali attività possono essere molto positive, stimolando il dialogo e la riflessione fra gli studenti e le studentesse. Se gli atti osservati si identificano come atti di bullismo o cyberbullismo, il docente e la scuola tutta devono intervenire seguendo il CASO B.

Nel CASO B, il/la docente deve:

- condividere immediatamente quanto osservato con il coordinatore di classe e con il referente per il bullismo e il cyberbullismo, valutando insieme le possibili strategie di intervento;
- avvisare la Dirigente Scolastica che convoca il Consiglio di classe (che applica il "Regolamento di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo nella scuola").

STRUMENTI DI SEGNALAZIONE PREVISTI DALL'ISTITUTO E CONTATTI UTILI

- scatola/box per la raccolta di segnalazioni anonime;
- sportello di ascolto psicologico.

Contatti utili:

- alfrilli.barbara@scuolecarduccilivorno.edu.it (Docente team prevenzione dei fenomeni di bullismo e cyberbullismo, secondaria di primo grado)
- pietrini.veronica@scuolecarduccilivorno.edu.it (Docente team prevenzione dei fenomeni di bullismo e cyberbullismo secondaria di primo grado)
- lanza.anna@scuolecarduccilivorno.edu.it (Docente team prevenzione dei fenomeni di bullismo e cyberbullismo secondaria di primo grado)
- pittalà.isabella@scuolecarduccilivorno.edu.it (Docente team prevenzione dei fenomeni di bullismo e cyberbullismo, primaria)
- barbieri.sara@scuolecarduccilivorno.edu.it (Docente team prevenzione dei fenomeni di bullismo e cyberbullismo, primaria)
- filieri.monica@scuolecarduccilivorno.edu.it (Docente team prevenzione dei fenomeni di bullismo e cyberbullismo, primaria)
- dirigente@scuolecarduccilivorno.edu.it (La Dirigente scolastica dell'IC Carducci)

5.3 GLI ATTORI SUL TERRITORIO

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

Si elencano gli attori sul territorio:

- **Comitato Regionale Toscana Per L' Unicef**

Via Vittorio Emanuele II, 303 50134 Firenze
E-mail: comitato.firenze@unicef.it Tel. 0552207144
Fax: 0550950129

- **Ufficio Scolastico Regionale Toscana**

Via Mannelli, 113, 50135 Firenze (FI)
Tel: (+39) 05527251
E-mail: https://www.miur.gov.it/web/miur-usr-toscana

- **Consultorio**

Via Peppino Impastato, 10 57100
Spazio famiglie mediazione familiare Tel: 0586 223627
Psicologo Tel: 0586 223607
Assistente sociale Tel: 0586 223607

- **Comando Carabinieri di Livorno**

Viale Fabbricotti, 157127 Livorno
Tel: 0586 551

- **Polizia Postale e delle Comunicazioni:**

https://www.commissariatodips.it/

- **Polizia postale Livorno**

Piazza Benamozegh,3 57123 Livorno
Tel: 0586276468

- **Garante per l'infanzia regione Toscana**

Palazzo Bastogi, via Cavour, 18 50129 Firenze
garante.infanzia@consiglio.regione.toscana.it
PEC consiglioregionale@postacert.toscana.it
Tel 055 2387802

5.4 ALLEGATI CON LE PROCEDURE

PROCEDURE INTERNE: COSA FARE IN CASO DI SOSPETTO CYBERBULLISMO?

Con nota prot. 5274 dell'11 luglio 2024, il Ministero dell'Istruzione e del merito ha fornito alle Istituzioni scolastiche, statali e paritarie, del primo ciclo di istruzione, disposizioni aggiornate in merito all'utilizzo degli smartphone e del registro elettronico. La comunicazione è consultabile sul sito web del MIM al link diretto https://www.miur.gov.it/-/disposizioni-in-merito-all-uso-degli-smartphone-e-del-registro-elettronico-nel-primo-ciclo-di-istruzione-a-s-2024-2025.

Divieto dell'uso dello smartphone a scopo didattico

A partire dall' anno scolastico 2024/2025, i cellulari saranno banditi dalle classi delle scuole dell'infanzia e del primo ciclo di istruzione, anche per le attività educative e didattiche.

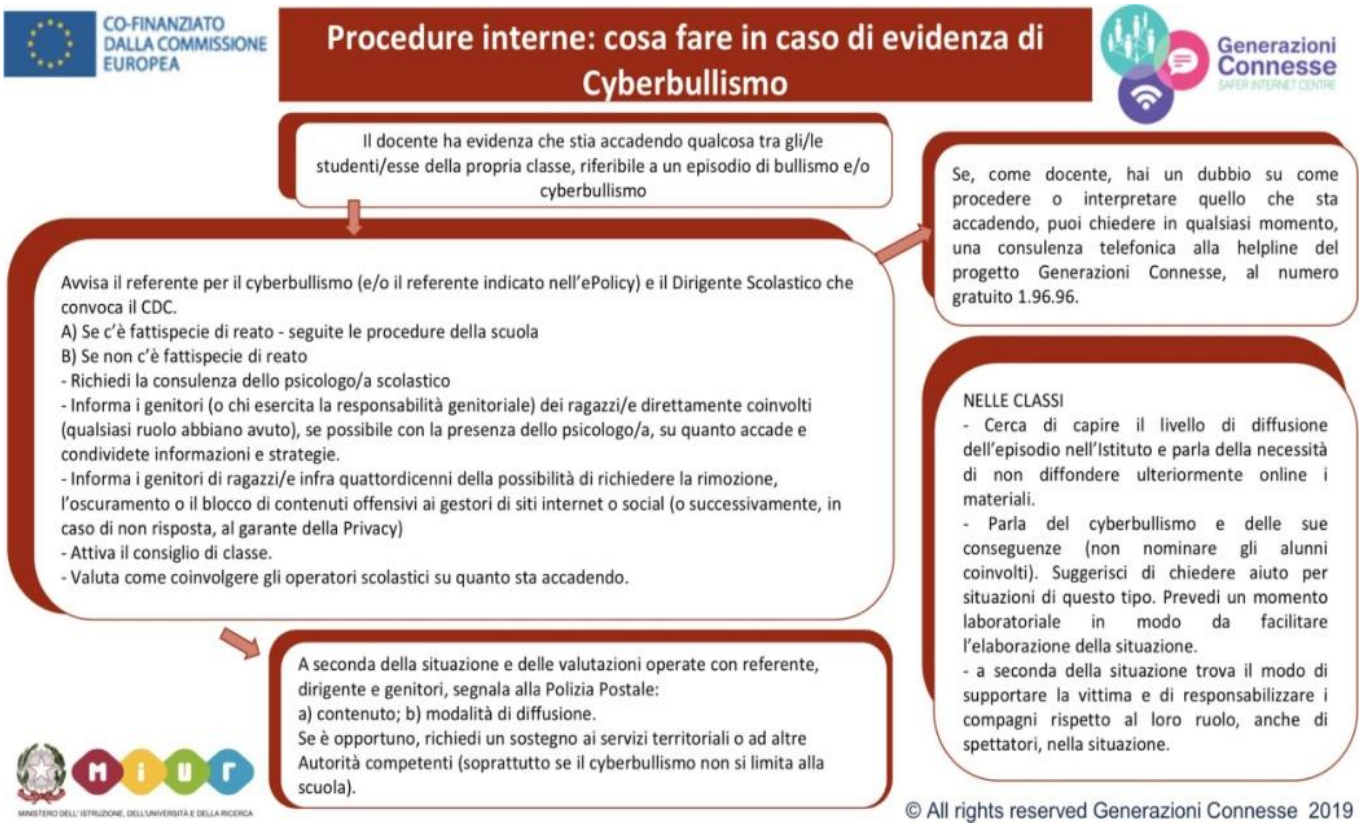
Il Ministro ha emanato una circolare che fornisce alle scuole indicazioni per introdurre il divieto dell'uso dello smartphone a scopo didattico. I rischi per la salute dei ragazzi che possono derivare dall'uso perdurante dei cellulari sono evidenziati dalla relazione finale, diffusa in allegato alla circolare, **dell'indagine conoscitiva realizzata nella scorsa legislatura dalla 7ª Commissione del Senato "Sull'impatto del digitale sugli studenti, con particolare riferimento ai processi di apprendimento".**

https://www.miur.gov.it/documents/20182/6739250/Documento_Senato_Sull%E2%80%99impatto_del_digitale_sugli_studenti.pdf/79d34842-4456-9aa3-7ae6-d22ab7d69312?t=1671527039119

La motivazione dietro questa scelta **è, dunque, la preoccupazione per l'impatto negativo che l'uso eccessivo dei cellulari può avere sul naturale sviluppo cognitivo dei ragazzi**.

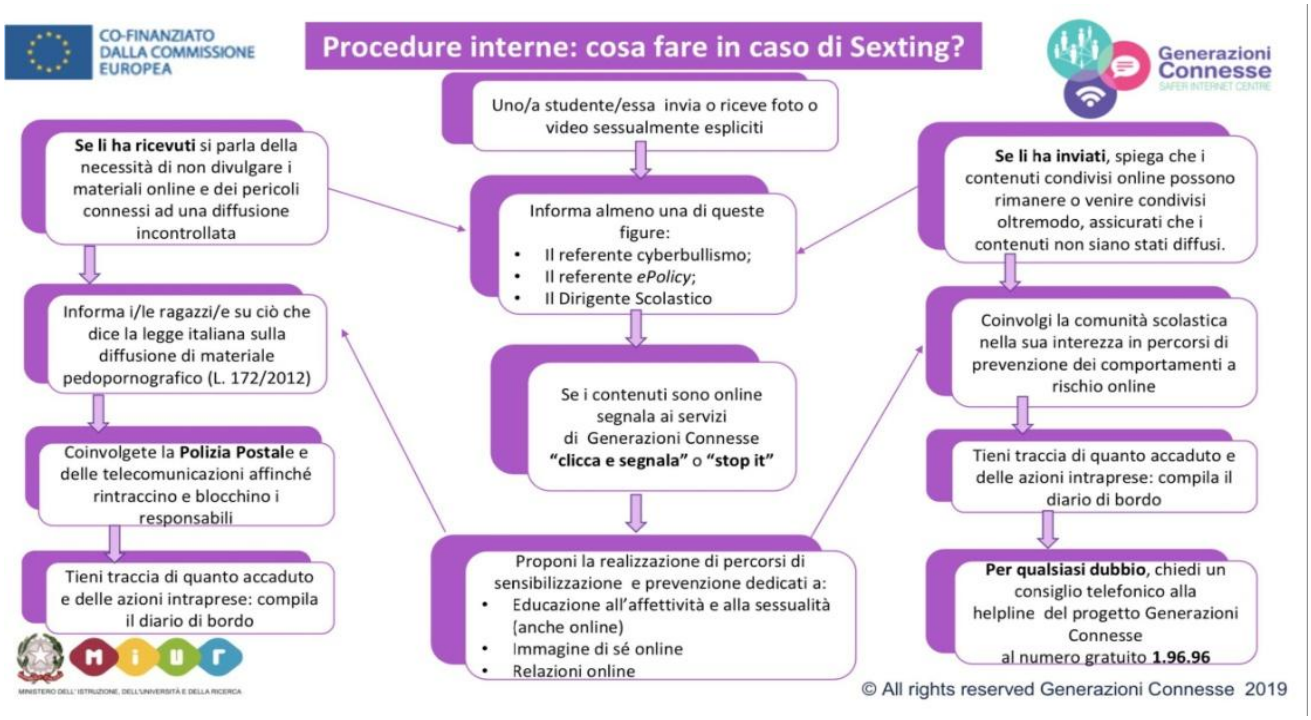
I più giovani sono perennemente connessi al *web*, perché «l'uso del digitale che ne fanno, prevalentemente *social* e videogiochi, favorisce il rilascio di dopamina, il neurotrasmettitore della sensazione di piacere». E c'è un nesso tra questo uso massiccio del digitale e «istigazione al suicidio, adescamento, *sexting*, bullismo, *revenge porn*: tutti reati in costante crescita», anche perché nelle "nuove piazze virtuali" «vige l'anonimato, i controlli sono scarsi, i minori vi si avventurano **senza alcuna sorveglianza da parte dei genitori**».

Per questo la Commissione sollecita «Parlamento e Governo ad individuare i possibili correttivi»: per esempio «favorire la riconoscibilità di chi frequenta il *web*;vietare l'accesso degli *smartphone* nelle classi; educare gli studenti ai rischi connessi all'abuso di dispositivi digitali e alla navigazione sul *web*; interpretare con equilibrio e spirito critico la tendenza epocale a sopravvalutare i benefici del digitale applicato all'insegnamento; incoraggiare, nelle scuole, la lettura su carta, la scrittura a mano e l'esercizio della memoria». Insomma, «governare e regolamentare quel mondo virtuale nel quale, secondo le ultime stime, i più giovani trascorrono dalle quattro alle sei ore al giorno». E — soprattutto — impedire la realizzazione di **quella che Aldous Huxley definì "dittatura perfetta"**: «Un sistema di schiavitù nel quale, grazie al consumismo e al divertimento, gli schiavi amano la loro schiavitù».


CO-FINANZIATO DALLA COMMISSIONE EUROPEA
Procedure interne: cosa fare in caso di evidenza di Cyberbullismo
Generazioni Connesse
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
Avvisa il referente per il cyberbullismo (e/o il referente indicato nell'ePolicy) e il Dirigente Scolastico che convoca il CDC.
A) Se c'è fattispecie di reato - seguite le procedure della scuola
B) Se non c'è fattispecie di reato
- Richiedi la consulenza dello psicologo/a scolastico
- Informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo/a, su quanto accade e condividete 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.
- Valuta come coinvolgere gli operatori scolastici su quanto sta accadendo.
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).
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
- Cerca di capire il livello di diffusione dell'episodio nell'Istituto e parla della necessità di non diffondere ulteriormente online i materiali.
- Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Suggerisci di chiedere aiuto per situazioni di questo tipo. Prevedi un momento laboratoriale in modo da facilitare l'elaborazione della situazione.
- a seconda della situazione trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.
MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
© All rights reserved Generazioni Connesse 2019


CO-FINANZIATO DALLA COMMISSIONE EUROPEA
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo
Generazioni Connesse
Il docente sospetta che stia accadendo qualcosa tra gli studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo
Sonda il clima di classe, ascoltando i ragazzi e monitorando ciò che accade (ma senza fare indagini o interrogatori).
Cerca di capire il livello di diffusione dell'episodio a livello di Istituto.
Condividi con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy): valuta con lui/loro le possibili strategie di intervento.
Valuta se è il caso di avvisare il consiglio di classe.
Valuta se è il caso 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.
Parla in classe del cyberbullismo e delle sue conseguenze (non nominare gli alunni che sospetti coinvolti). Suggerisci di chiedere aiuto per situazioni di questo tipo.
Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)
Se emergono evidenze passa allo schema successivo
Informa i/le ragazzi/e su ciò che dice la legge italiana su cyberbullismo L. 71/2017)
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano
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
MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
© All rights reserved Generazioni Connesse 2019

PROCEDURE INTERNE: COSA FARE IN CASO DI SEXTING?



PROCEDURE INTERNE: COSA FARE IN CASO DI ADESCAMENTO ONLINE?