

 Ministero dell'Istruzione e del Merito	Istituto Comprensivo di Cisano Bergamasco (Caprino, Pontida, Torre de' Busi) Infanzia - Primaria - Secondaria di primo grado 24034 Cisano Bergamasco (BG) Via Giovanni Pascoli, 5 bgic841003@pec.istruzione.it bgic841003@istruzione.it C.F.91025960161 cod. univoco UFI0JO Tel: 035781363 Fax: 035781083 www.comprensivocisano.gov.it	Plessi: Infanzia di Caprino Infanzia di Cisano Primaria di Caprino Primaria di Cisano Primaria di Pontida Primaria di Torre de' Busi Secondaria 1° gr. Caprino Secondaria 1° gr. Cisano Secondaria 1° gr. Pontida Secondaria 1° gr. Torre de' Busi
---	--	--

E-POLICY D'ISTITUTO

1. INTRODUZIONE

Lo sviluppo e l'integrazione dell'uso delle TIC (tecnologie dell'informazione e della comunicazione) nella didattica, nonché la presenza sempre più diffusa delle tecnologie digitali nella vita di tutti i giorni, pongono nuove attenzioni dal punto di vista del loro uso sicuro, consapevole e positivo. Vi sono numerose evidenze scientifiche sui benefici che l'uso delle tecnologie digitali può apportare nel processo di insegnamento/apprendimento. È compito dell'intera comunità scolastica, genitori inclusi, garantire che gli studenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro. È in questo quadro che si inserisce la necessità di dotare la Scuola di una propria Policy di E-safety, nell'ottica della gestione delle infrazioni attraverso il monitoraggio continuo della Policy e dell'integrazione con il Regolamento d'Istituto.

Obiettivo del documento è quello di educare e sensibilizzare l'intera comunità scolastica all'uso sicuro e consapevole di internet in conformità con le "Linee di Orientamento" (Registro Decreti 0000018. 13-01-2021) per azioni di prevenzione e di contrasto al bullismo e cyberbullismo elaborate

dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con il Safer Internet Center per l'Italia, programma comunitario istituito dal Parlamento Europeo e dal Consiglio dell'Unione. Il documento potrà essere revisionato annualmente.

1.A RUOLI E RESPONSABILITÀ

La capacità di partecipare in modo costruttivo e consapevole alle comunità online e ai network virtuali costituisce un prerequisito fondamentale per partecipare in modo attivo alla società della conoscenza e dell'informazione. Alla diffusione dei nuovi media e degli strumenti del web 2.0 si accompagna, infatti, l'emergere di nuove opportunità di partecipazione civica e sociale (e-engagement, e-inclusion), che richiedono capacità comunicative e socio-relazionali adeguate. È fondamentale quindi conoscere come ci si comporti in queste comunità, quali regole vadano rispettate e quali ruoli e responsabilità abbiano i soggetti che vi partecipano. La scuola, nel farsi carico della formazione globale dell'individuo nella sua fase evolutiva, deve individuare in maniera chiara e inequivocabile ruoli e responsabilità di ciascuno degli attori del percorso formativo.

Nella promozione dell'uso consapevole della rete

Il Dirigente Scolastico deve:

- garantire la corretta formazione del personale scolastico sulle tematiche relative all'uso sicuro e consapevole di internet e della rete;
- garantire una formazione adeguata del personale docente relativo all'uso delle TIC nella didattica;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

L'animatore digitale, supportato dal Team dell'innovazione, deve:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e coordinare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale".

Il direttore dei servizi generali e amministrativi deve:

- assicurare, 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;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, registro elettronico, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

I docenti devono:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;

- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni comprendano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- assicurare che gli alunni 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 sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, fotocamere, ecc. di proprietà dell'Istituto da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta inadeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare 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 di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente scolastico e ai genitori 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.

Gli alunni devono:

- 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 TIC per la ricerca di contenuti e materiali ma anche 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, onde evitare il rischio di commettere furto di dati personali, anche quando altri account siano erroneamente lasciati attivi sui terminali della scuola;
- riporre particolare cura nella gestione delle password personali, specialmente per quanto riguarda l'account d'Istituto;
- 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 ai genitori.

I genitori devono:

- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC nella didattica;
- seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti;
- 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.

Dal 14 giugno 2024 è entrato in vigore il provvedimento ministeriale relativo alla Legge n° 70 sulla prevenzione dei fenomeni di bullismo e cyberbullismo del 17 maggio 2024: "ogni istituto scolastico, nell'ambito della propria autonomia e in conformità alle linee di orientamento di cui al comma 1, adotta un codice interno per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo e istituisce un **tavolo**

permanente di monitoraggio del quale fanno parte rappresentanti degli studenti, degli insegnanti, delle famiglie ed esperti di settore”. Si riporta, di seguito, il link alla Gazzetta Ufficiale con il testo completo: <https://www.gazzettaufficiale.it/eli/id/2024/05/30/24G00086/SG>.

1.B CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA

La scuola dovrà assicurare promozione della condivisione degli intenti esplicitati nel documento in modo tale che:

- tutti gli alunni siano informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dai docenti e utilizzati solo con la loro autorizzazione;
- uno o più moduli di insegnamento sulla e-safety siano programmati nell'ambito delle diverse discipline per l'acquisizione della consapevolezza di un uso sicuro e responsabile di internet;
- l'elenco delle regole per la sicurezza on-line sia pubblicato in tutte le aule o laboratori con accesso a internet;
- la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet venga discussa negli organi collegiali (Consigli di classe, Collegio dei Docenti, Consiglio d'Istituto) e comunicata a tutto il personale con il presente documento;
- il personale docente venga reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato;
- una adeguata formazione dei docenti sull'uso sicuro e responsabile di internet professionalmente e personalmente sia assicurata a tutto il personale;
- il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC venga supervisionato dall'Animatore digitale che segnalerà al DSGA eventuali problemi che dovessero richiedere interventi di tecnici.
- l'Animatore digitale e il Team Innovazione mettano a disposizione dei docenti il proprio know-how;
- tutto il personale sia consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile;

- 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 TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;
- l'Animatore digitale fornirà ai genitori 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 ai genitori 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;
- i genitori esperti potranno collaborare nelle attività di informazione/formazione del personale e degli alunni.

1.C GESTIONE DELLE INFRAZIONI ALLA POLICY

Le potenziali infrazioni a carico degli alunni sono identificabili in:

- uso di social network e blog per pubblicare, condividere o, in genere, postare commenti o giudizi offensivi della dignità altrui;
- condivisione di dati personali che possano permettere l'identificazione;
- connessioni a siti proibiti o comunque non autorizzati;
- pubblicazione di foto o immagini non autorizzate e/o compromettenti.

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo del discente coerente con quanto definito nel Regolamento d'Istituto, nella sezione INFRAZIONI E SANZIONI DISCIPLINARI.

Un primo intervento viene attuato dal docente secondo le modalità indicate:

- richiamo verbale;
- richiamo verbale con annotazione disciplinare sul registro e sul diario personale;

- convocazione della famiglia.

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

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e una custodia inadeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato degli strumenti digitali.

Il Dirigente scolastico può controllare l'utilizzo degli strumenti digitali per verificarne la conformità alle regole di sicurezza, come l'accesso a internet, ma non alla posta elettronica personale, cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservando una copia per eventuali successive investigazioni come in caso di contenzioso. Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla Legge e dai contratti di lavoro.

Disciplina dei genitori

In considerazione dell'età dei discenti, le azioni e la condotta dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola.

Le situazioni familiari meno favorevoli sono:

- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo dello smartphone;
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- un utilizzo del PC in comune con gli adulti che possono conservare in memoria materiali non idonei. I genitori degli alunni possono essere convocati a scuola per concordare misure educative sanzionatorie anche a norma di legge.

1.D MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche ai docenti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti. L'aggiornamento della policy sarà curato dal Dirigente scolastico, dall'Animatore digitale, del Team Innovazione e dagli Organi Collegiali, a seconda degli aspetti considerati.

1.E INTEGRAZIONE DELLA POLICY CON REGOLAMENTI ESISTENTI

Sebbene l'attuale Regolamento di Istituto con relativa integrazione del Regolamento speciale internet risulti essere esaustivo nella sua articolazione in materia di sicurezza, la scuola si riserva di intervenire con modifiche e/o integrazioni.

2. FORMAZIONE E CURRICOLO

L'impiego delle TIC è senz'altro un fattore di innovazione della didattica, di aumento della motivazione e del rendimento degli studenti. Tuttavia, non è possibile risolvere una questione di tipo didattico esclusivamente su un piano tecnologico. È, invece, auspicabile una modifica delle pratiche tradizionali di insegnamento. Infatti, non è più sufficiente possedere la dotazione tecnologica, ma è fondamentale l'effettivo utilizzo che ne viene

fatto e quindi la capacità di comprenderne le potenzialità rispetto a contesti e finalità specifici. Per sostenere questo processo all'interno della scuola è stato necessario investire sulla formazione e l'aggiornamento degli insegnanti, soprattutto in relazione alla didattica per competenze.

2.A CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

Il concetto di didattica per competenze ha assunto un ruolo centrale in ambito europeo. Nel 2006, il Parlamento Europeo ha elaborato una Raccomandazione (2006/962/CE) in cui delinea il quadro delle competenze necessarie per il lifelong learning, ovvero competenze necessarie per esercitare pienamente il diritto di cittadinanza nella Società Contemporanea. L'Italia ha progressivamente recepito il quadro comunitario dando vita a un processo di riforma educativa. Il tema della competenza digitale (digital literacy) è emerso all'interno del dibattito internazionale sul lifelong learning, ovvero sulla definizione dei saperi chiave per vivere attivamente nella cosiddetta Società dell'Informazione, un contesto che richiede un nuovo modello di alfabetizzazione in cui le nuove tecnologie e la rete possono essere considerati veri e propri vettori di partecipazione e la competenza digitale è quindi annoverata tra i sapere necessari per la cittadinanza.

Ma cosa significa essere competenti quando parliamo di TIC? Istintivamente si pensa ad abilità informatiche di base quali saper utilizzare il computer, conoscere specifici software o servizi web, possedere uno smartphone. Tuttavia, se proviamo a rispondere alla stessa domanda ponendoci in un'ottica pedagogica e partecipativa, penseremo probabilmente anche ad altre capacità come quella di saper cercare e selezionare le informazioni online, oppure saper lavorare in maniera collaborativa a distanza, tutelare la propria privacy nei social network e altre ancora. Questo semplice esercizio – che potremmo ripetere anche in classe con i nostri studenti – ci porta a considerare riduttiva una definizione di digital literacy come expertise tecnica, mettendo in luce le implicazioni cognitive e relazionali: diventa opportuno pensare la competenza digitale come un costrutto complesso, in cui si intersecano dimensioni di natura diversa, che potremmo così schematizzare:

- **Dimensione tecnologica:** questo ambito fa riferimento a una serie di skills tecnologiche di base, come ad esempio la conoscenza di dispositivi e interfacce, ma comprende anche livelli più avanzati legati alla capacità di valutare le potenzialità dei contesti tecnologici in trasformazione, imparando a selezionare le soluzioni più opportune per affrontare ciascun compito;

- **Dimensione cognitiva:** comprende abilità legate al trattamento dell'informazione, dalla capacità di accedere, selezionare e interpretare dati a quella di valutarne criticamente la pertinenza e l'affidabilità, ma anche il saper trattare testi e dati per produrne sintesi, analisi e rappresentazioni con tabelle e grafici;
- **Dimensione etica:** questa dimensione riguarda il saper interagire con gli altri in modo corretto e responsabile, la circolazione del sapere online e il rispetto dei diritti di proprietà intellettuale, il tema dell'accessibilità e dell'inclusione. Comprende alcune delle tematiche più attuali rispetto al tema delle nuove tecnologie, dalla tutela della privacy al contrasto del fenomeno del cyberbullismo, e quelle che riguardano la dimensione relazionale ed affettiva dell'utilizzo di internet: il fatto di non vedersi e di non sentirsi direttamente, o di non entrare in contatto visivo, abbassa timidezze e inibizioni, per cui spesso nella comunicazione in rete si raggiungono elevati livelli di confidenza e intimità e a volte, di seduttività, proprio perché l'altro/a può essere uno sconosciuto e come tale, liberamente immaginato e idealizzato.

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

Da ciò è emersa la necessità di individuare e di certificare, al termine del percorso scolastico, coerentemente con quanto normato dalla C.M. n 3, prot. n. 1235 del 13 febbraio 2015, le competenze digitali, intese come competenze chiave, che i discenti devono acquisire. Ne è derivato il seguente profilo:

Usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo.

Il livello raggiunto è identificato dagli indicatori:

- A. Avanzato: L'alunno/a svolge compiti e risolve problemi complessi, mostrando padronanza nell'uso delle conoscenze e delle abilità; propone e sostiene le proprie opinioni e assume in modo responsabile decisioni consapevoli.
- B. Intermedio: L'alunno/a svolge compiti e risolve problemi in situazioni nuove, compie scelte consapevoli, mostrando di saper utilizzare le conoscenze e le abilità acquisite.
- C. Base: L'alunno/a svolge compiti semplici anche in situazioni nuove, mostrando di possedere conoscenze e abilità fondamentali e di saper applicare basilari regole e procedure apprese.
- D. Iniziale: L'alunno/a, se opportunamente guidato/a, svolge compiti semplici in situazioni note.

2.B SENSIBILIZZAZIONE DELLE FAMIGLIE

In considerazione dell'importanza di favorire la sinergia degli interventi educativi di scuola e famiglia per il successo scolastico ed educativo di ogni studente, il presente documento, assieme al Patto Educativo di Corresponsabilità stipulato con le famiglie degli alunni quale l'impegno reciproco di scuola e famiglia alla corresponsabilità formativa, nella quale rientrano a pieno titolo i temi legati alla eSafety, è a disposizione delle famiglie sul sito web d'Istituto. Allo scopo di mantenere viva l'attenzione delle famiglie su tali temi, verranno inoltre valorizzate le opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità. Il coinvolgimento dell'intera Comunità scolastica è parte integrante del PTOF ed è una delle misure individuate nel Piano d'azione proposto a "Generazioni Connesse". Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di smartphone, chat line e social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Si prevede la creazione di una bacheca virtuale sul sito scolastico istituzionale per la condivisione di materiali dedicati al tema del Web sicuro.

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE T.I.C. DELLA SCUOLA

L'infrastruttura e la strumentazione TIC dell'Istituto sono un patrimonio di tutti, esse vanno utilizzate nel rispetto delle norme contenute nel "Regolamento per l'utilizzo dei laboratori multimediali". I danni causati alle attrezzature saranno a carico di chiunque disattenda il suddetto Regolamento. L'accesso ad infrastrutture e strumentazione TIC utilizzabili per la didattica è riservato ai docenti e agli alunni ed è limitato al perseguimento di scopi formativi. I docenti devono formare i propri alunni al rispetto del suddetto Regolamento, per gli aspetti di loro pertinenza.

La scuola deve considerare l'ambiente online alla stregua dell'ambiente fisico e valutare tutti gli aspetti legati alla sicurezza nel momento in cui permette l'accesso alla rete tramite i collegamenti scolastici. Un aggiornamento delle infrastrutture prevederà nel breve termine l'accesso a internet a tutte le classi attraverso una rete WI-FI adeguata al numero di studenti.

L'infrastruttura quindi non va più pensata solamente come hardware e rete (wireless e non), ma occorre anche considerare tutti gli aspetti che riguardano la gestione degli account degli utenti (in modo differenziato tra studenti e insegnanti), il filtraggio dei contenuti e gli aspetti legali che riguardano prevalentemente la privacy.

3.A ACCESSO AD INTERNET: FILTRI, ANTIVIRUS E SULLA NAVIGAZIONE

Tutti i plessi della scuola, dall'Infanzia alla Secondaria di Primo Grado, sono dotati di collegamento internet e wifi, Firewall, antivirus (si veda il PTOF d'Istituto).

3.B GESTIONE ACCESSI (PASSWORD, BACKUP, ECC.)

La scuola adotta tutte le necessarie precauzioni per evitare l'accesso a siti non adatti all'interno della scuola. Questo avviene attraverso l'adozione di firewall. L'accesso ai portali istituzionali come SIDI, Istanze on-line, alla Segreteria Digitale, PON ecc. prevede l'uso di credenziali personali, mentre l'accesso a portali tematici si effettua per mezzo di password uniche condivise tra i referenti di progetti e/o azioni e la dirigenza. I docenti possono accedere alla propria sezione del registro elettronico con credenziali personali. Anche a genitori e alunni sono fornite credenziali personali

di accesso al registro elettronico. Il backup viene eseguito dal sistema periodicamente e i dati preservati in cloud. I dati personali vengono trattati nel rispetto della normativa sulla privacy.

3.C REGISTRO ELETTRONICO

L'Istituto assegna a ciascun docente e a ciascuna famiglia le credenziali username e password per l'accesso al registro elettronico sulla piattaforma Argo. Ciascun docente è tenuto ad aggiornare il registro personale secondo le direttive stabilite dalla Dirigenza. I genitori degli alunni sono altresì tenuti ad accedere regolarmente al registro elettronico per monitorare costantemente il rendimento didattico-disciplinare dei propri figli.

3.D E-MAIL

L'accesso alla posta elettronica istituzionale MIUR può essere effettuato solo dal personale di segreteria e dalla presidenza utilizzando credenziali uniche. L'uso di e-mail personali viene favorito come mezzo di diffusione di comunicati e notifiche di circolari d'Istituto pubblicate sul sito istituzionale.

La Scuola ha dotato tutto il suo personale, docente e non docente, e i suoi alunni di un account Google d'istituto, avente come dominio il seguente: "@comprensivocisano.edu.it". L'utilizzo di un'email d'istituto ha reso più agile la comunicazione interscolastica e permesso di uniformare i canali comunicativi. Ad inizio ciclo scolastico i genitori sottoscrivono un regolamento di utilizzo ed una liberatoria relativa alla mail d'Istituto mentre a conclusione del ciclo scolastico l'Istituto provvederà all'eliminazione delle utenze, così pure in caso di trasferimento di alunni in altra scuola.

3.E SUITE GOOGLE

Insieme all'indirizzo email, l'account Google "@comprensivocisano.edu.it" fornisce a tutto il personale e agli studenti un insieme di altri strumenti digitali:

- Google Meet, per riunioni e lezioni in videoconferenza;

- Google Drive, che fornisce uno spazio di archiviazione illimitato;
- Google Classroom, per la realizzazione di classi virtuali.

Il 28 febbraio 2023 Google ha annunciato la crittografia lato client anche su Google Workspace per il miglioramento della sicurezza sulla privacy dei dati di Gmail e Calendar. La normativa introdotta da Google riguarda anche l'autorizzazione per le app di terze parti che verrà richiesta a maggiore tutela della privacy per tutte le attività con finalità didattiche.

3.F SITO WEB DELLA SCUOLA

La scuola è dotata di un sito istituzionale, tramite il quale è facilmente possibile accedere al contenuto di proprio interesse (Pubblicità legale, circolari, bacheca sindacale ecc) anche attraverso siti tematici. Sul sito è possibile trovare Regolamenti, materiali didattici, pubblicizzazione di eventi, documentazione di attività curricolari ed extracurricolari svolte. Pulsanti attivi permettono l'accesso a link di interesse tra cui il Registro Elettronico. Il sito è aggiornato quotidianamente dalla Funzione Strumentale preposta.

3.G SOCIAL NETWORK

Attualmente l'Istituto non possiede pagine Facebook o Instagram.

3.H PROTEZIONE DEI DATI PERSONALI

Nell'epoca della condivisione, in cui il confine tra pubblico e privato sembra essere costantemente messo in discussione, è necessario imparare a gestire i propri dati sensibili e a tutelarli, anche alla luce delle strategie di web marketing e profilatura dell'utente. Per questo motivo il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione).

Le nuove tecnologie della comunicazione, dai blog ai wiki, ai social network, consentono di condividere pubblicamente le informazioni personali e ciò solleva nuove e pressanti questioni per la tutela della privacy e dei dati sensibili. Molti giovani, ma anche i genitori e gli adulti in genere,

condividono con disinvoltura informazioni personali su siti e social network, accessibili al largo pubblico come Facebook. Oltre al problema dell'esposizione dei dati sensibili, vi è quello del tracciamento delle informazioni personali dell'utente per usi commerciali. Le strategie di web marketing si basano infatti sulla possibilità di conoscere e delineare un profilo preciso dell'utente attraverso il tracciamento delle sue azioni e di utilizzare gli utenti stessi come generatori e promotori di contenuti pubblicitari. Per un uso consapevole e sicuro dei nuovi media, in particolare Internet, occorre allora rendere le persone capaci di gestire in modo selettivo e pertinente le informazioni condivise elettronicamente. Per questo motivo ai genitori viene fornita una informativa sul trattamento dei dati personali ai sensi dell'Art. 13 del Reg. Ue 2016/679, e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, come ad esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome e la voce del proprio figlio/a, all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della Scuola. A tale proposito si evidenzia che le immagini e le riprese audio-video realizzate dalla scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della scuola tramite il sito internet di Istituto, pubblicazioni, mostre, corsi di formazione, seminari, convegni e altre iniziative promosse dall'Istituto anche in collaborazione con altri enti pubblici. L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la propria dignità personale ed il decoro e comunque per uso e/o fini diversi da quelli sopra indicati.

4. STRUMENTAZIONE PERSONALE

4.A PER GLI STUDENTI: GESTIONE DEGLI STRUMENTI PERSONALI

Dall'anno scolastico 2024/25 non è consentito agli alunni l'utilizzo del telefono cellulare a scuola, come da recente disposizione ministeriale.

Si riporta di seguito il link ufficiale alla normativa di riferimento:

<https://www.mim.gov.it/-/disposizioni-in-merito-all-uso-degli-smartphone-e-del-registro-elettronico-nel-primo-ciclo-di-istruzione-a-s-2024-2025>.

L'unica eccezione riguarda gli alunni con bisogni educativi speciali, per i quali l'uso dello smartphone può essere autorizzato come strumento compensativo, se previsto dal Piano Educativo Individualizzato (PEI) o dal Piano Didattico Personalizzato (PDP)

Solo in caso di comprovate necessità di organizzazione familiare e relativa documentazione scritta richiesta all'Istituto, gli alunni potranno portare il telefono nell'ambiente scolastico che dovrà essere custodito dagli interessati rigorosamente spento durante tutto l'arco di tempo a scuola e in ogni ambiente della stessa, come già precedentemente indicato dalla Direttiva Ministeriale n. 30 del 15 marzo 2007. Ai sensi della Direttiva Ministeriale n. 30 del 15 marzo 2007, con la condivisione della presente Policy, "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone" a seguito di violazioni della presente policy. In base al Regolamento Disciplinare vigente presso l'Istituto, qualsiasi utilizzo improprio del dispositivo cellulare durante l'orario scolastico si configura come mancanza grave e, come tale, è punibile con sanzioni che possano prevedere finanche la sospensione dalle attività didattiche. Sarà il Consiglio di Classe, congiuntamente al Dirigente Scolastico, a comminare la sanzione in relazione alla gravità dell'atto commesso.

4.B PER I DOCENTI: GESTIONE DEGLI STRUMENTI PERSONALI

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili. Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali, per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

4.C PER IL PERSONALE DELLA SCUOLA: GESTIONE DEGLI STRUMENTI PERSONALI

Tutto il personale scolastico è autorizzato ad utilizzare device personali laddove non stia assolvendo ad un ruolo didattico, a condizione che l'utilizzo non intralci il normale svolgimento delle attività scolastiche, né distraiga dal corretto svolgimento delle proprie mansioni. In tal caso la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente al proprietario.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

PREVENZIONE

Per i ragazzi nativi digitali le interconnessioni tra vita e tecnologia sono la normalità. Essi, pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti e tale fenomeno è tanto maggiore quanto è più forte il coinvolgimento emotivo nell'utilizzo dei nuovi media. Le tecnologie digitali offrono da tempo la possibilità di ampliare la propria rete di amicizie in modo quasi smisurato: non è infrequente che gli adolescenti "si sfidino" tra loro rispetto al numero di "amicizie" strette online. Avere molti amici nella vita virtuale, o molti followers, è elemento di grande popolarità e di vanto con gli amici della vita reale. Non a caso, quindi, gli adolescenti aggiungono tra le proprie cerchie, in particolare sui loro profili social, "amici di amici" senza valutare attentamente a chi stanno dando accesso alle proprie informazioni, alle proprie foto, spesso ai luoghi che frequentano, a quello che viene chiamato "diario virtuale". Tra le poche accortezze che molti ragazzi utilizzano per valutare l'affidabilità e la sicurezza di chi chiede loro di essere aggiunto tra gli amici, c'è quella di valutare il numero di amici in comune con la persona che aggiungono. Se per molti adulti sono evidenti l'ingenuità e l'imprudenza con cui bambini e adolescenti si avvicinano a questa modalità di relazione e amicizia "online", per altri adulti e per i ragazzi stessi non è così. Questo li espone a rischi notevoli: tra gli altri, quello di condividere con sconosciuti l'accesso al loro mondo online, e quindi alle informazioni che potrebbero essere utilizzate in modo inaspettato e non sempre positivo. Aiutare i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, è allora un compito importante anche dell'insegnante che contribuisce in questo modo alla loro tutela nella vita virtuale, con ripercussioni non banali nella vita reale. Tra i principali rischi, sia di carattere comportamentale che di matrice tecnica, ricordiamo:

- possibile esposizione a contenuti violenti e non adatti alla loro età;
- videogiochi diseducativi;
- pubblicità ingannevoli;

- accesso ad informazioni scorrette (fake news);
- virus informatici in grado di infettare computer e cellulari;
- possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e (adescamento);
- rischio di molestie o maltrattamenti da coetanei (cyber-bullismo);
- scambio di materiale a sfondo sessuale (sexting);
- uso eccessivo di Internet/cellulare (dipendenza);
- adescamento on-line (grooming).

È opportuno che i docenti, nell'espletamento delle proprie funzioni di formatori ed educatori sappiano cogliere ogni opportunità per riflettere insieme agli alunni sui tali rischi. Fondamentale è monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente, anche mediante il ricorso alle figure di sistema specializzate, per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'instaurazione di un clima positivo, di reciproca accettazione e rispetto, nelle situazioni di difficoltà socio-relazionale. Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i temi sopra menzionati, cui la scuola porrà particolare attenzione, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità. L'Istituto si impegna, infatti, a promuovere ad ogni livello percorsi educativi circa il corretto utilizzo delle tecnologie e il rispetto reciproco per gli studenti, oltre che incontri formativi rivolti ai genitori, per fornire loro le indicazioni essenziali circa i pericoli incontrati dai loro figli in rete. Tutto ciò per permettere una maggiore sinergia tra scuola e famiglia essenziale per una prevenzione efficace di atti di bullismo e cyberbullismo. Data la capillare diffusione degli strumenti digitali e della precocità con cui i nostri ragazzi, nativi digitali, si affacciano al mondo dei social, è necessario mettere in pratica azioni di prevenzione fin dalla Primaria, in particolare dalla classe terza in poi.

RILEVAZIONE

Laddove il docente colga possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati nel paragrafo “Prevenzione”, dovrà informare il referente bullismo, se si tratta di un CASO SOSPETTO; sarà tenuto ad informare invece il Dirigente scolastico e il referente bullismo di fronte a una EVIDENZA. Le segnalazioni potranno avvenire mediante la compilazione di una “scheda di segnalazione” (di seguito allegata e disponibile nell’area riservata del sito web istituzionale), che potrà essere aggiornata periodicamente nei Consigli di Classe. Posto che il primo e più efficace strumento di individuazione, resta l’osservazione del gruppo classe durante le attività didattiche da parte del docente. Va precisato che la rilevazione dei casi è comunque compito dell'intera comunità scolastica: non solo insegnanti, ma anche educatori, personale ATA. Va tenuto altresì presente che, onde prevenire confusioni o errate segnalazioni, per “atto di bullismo” è da intendersi “un’azione continuativa e persistente che mira deliberatamente a far del male o danneggiare qualcuno”. La modalità diretta si manifesta in prepotenze fisiche e/o verbali. La forma indiretta di prevaricazione riguarda una serie di dicerie sul conto della vittima, l'esclusione dal gruppo dei pari, l'isolamento, la diffusione di calunnie e di pettegolezzi e altre modalità definite di "cyberbullying" inteso quest'ultimo come particolare tipo di aggressività intenzionale agita attraverso forme elettroniche” (Direttiva Ministeriale n.16 del 5 febbraio 2007). Per quanto riguarda più nello specifico del “cyberbullismo”, invece, “si intende 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” (L. n. 71 del 29 maggio 2017). Onde prevenire episodi di cyberbullismo, l’Istituto ha proposto una serie di strumenti che permettano un migliore monitoraggio. Tra queste la creazione di uno sportello “virtuale” di denuncia per gli studenti, anche i più timidi, che possono così segnalare eventuali episodi superando le proprie paure. Lo sportello è attivo al seguente indirizzo, cyberbullismo@comprensivocisano.edu.it, il quale sarà gestito dal referente bullismo e dai membri della commissione “Cyberbullismo”.

GESTIONE DEI CASI

Caso sospetto

A seguito della segnalazione, il docente e il referente del cyberbullismo valutano possibili strategie di intervento. Per i casi sospetti, il docente è invitato a:

- valutare se sia il caso di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate;
- dialogare con i colleghi/e: confrontarsi, condividendo le proprie preoccupazioni;
- raccogliere le informazioni, ascoltando i ragazzi e monitorando ciò che accade;
- capire il livello di diffusione dell'episodio a livello di Istituto.

Sarà inoltre importante il dialogo con la classe, in quanto il bullismo non è mai un episodio che coinvolge il solo individuo, ma che ha ampie ricadute sul gruppo-classe. Il docente, pertanto, è tenuto a dialogare con la classe, parlando di bullismo, di cyberbullismo e delle loro conseguenze. Suggerisce di chiedere aiuto per situazioni di questo tipo; prevede un momento laboratoriale; se ancora non ci sono evidenze, è importante prevenire e lavorare con la classe sul clima e sulle dinamiche.

Evidenza

A seguito della segnalazione, il Dirigente Scolastico avrà cura di contattare il docente per un colloquio finalizzato a valutare la necessità di effettuare uno o più interventi di osservazione in classe e, successivamente, di pianificare adeguati interventi educativi e, ove necessario, di coinvolgere le famiglie per l'attivazione di un percorso comune e condiviso di sostegno al disagio. Le azioni poste in essere dalla scuola saranno dirette non solo a supportare le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, ma anche a realizzare

interventi educativi rispetto a quanti abbiano messo in atto comportamenti lesivi, ove si tratti di soggetti interni all'Istituto. In particolare il Dirigente, in accordo con il Consiglio di Classe:

- 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);
- valuta come coinvolgere gli operatori scolastici su quanto sta accadendo.

Nei casi di maggiore gravità si valuterà anche il coinvolgimento di attori esterni quali le forze dell'ordine e i servizi sociali.

A seconda della situazione e delle valutazioni operate con il referente, i docenti del CdC e i genitori, in caso di grave atto di cyberbullismo, si segnalerà l'episodio alla Polizia Postale indicando:

- a) contenuto;
- b) modalità di diffusione.

 Ministero dell'Istruzione e del Merito	Istituto Comprensivo di Cisano Bergamasco (Caprino, Pontida, Torre de' Busi) Infanzia - Primaria - Secondaria di primo grado 24034 Cisano Bergamasco (BG) Via Giovanni Pascoli, 5 bgic841003@pec.istruzione.it bgic841003@istruzione.it C.F.91025960161 cod. univoco UFI0JO Tel: 035781363 Fax: 035781083 www.comprensivocisano.gov.it	Plessi: Infanzia di Caprino Infanzia di Cisano Primaria di Caprino Primaria di Cisano Primaria di Pontida Primaria di Torre de' Busi Secondaria 1° gr. Caprino Secondaria 1° gr. Cisano Secondaria 1° gr. Pontida Secondaria 1° gr. Torre de' Busi
---	--	--

SCHEDA PER L'INDIVIDUAZIONE/MONITORAGGIO DEI FATTI PRESUNTI O TALI DI BULLISMO E CYBERBULLISMO

INDIVIDUAZIONE DEL CASO

La presente scheda è a carico del Coordinatore di classe che raccoglie tutte le informazioni da alunni, genitori, docenti e personale Ata.

Se necessario, **COMPIE SEGNALAZIONE** al Dirigente scolastico.

ANALISI DEL PROBLEMA E AZIONI PROGRESSIVE

- 1) Incontri individuali con alunni e genitori degli alunni coinvolti (verbalizzare e far sottoscrivere alla famiglia. Valutare presenza Dirigente scolastico o preposti, specialisti e/o Referente bullismo e cyberbullismo).
- 2) Riunione del Consiglio di Classe per definire e valutare il caso. (Valutare presenza Dirigente scolastico o preposti, specialisti e/o Referente bullismo e cyberbullismo).
- 3) Riunione eventuale del Consiglio di Classe allargato ai genitori coinvolti o tutti. (Valutare presenza Dirigente scolastico o preposti, specialisti e/o Referente bullismo e cyberbullismo).

- 4) Valutazione della possibilità di coinvolgimento dell'Interclasse per monitorare e sostenere gli interventi successivi.

DEFINIZIONE INTERVENTI INDIVIDUALIZZATI IN GRADUALITÀ

- 1) Ascolto e dialogo individuale con gli alunni coinvolti.
- 2) Confronto e discussione tra i protagonisti.
- 3) Discussione in classe per ristabilire le regole di comportamento.
- 4) Letture e questionari attinenti alle problematiche verificatesi.
- 5) Riflessioni scritte, lettera di scuse, (attore principale bullismo/cyberbullismo), di richieste (vittima), di riflessione sul proprio ruolo (spettatori passivi, gregari...). Eventuali incontri protetti tra attori per ricostruire la dinamica.
- 6) Elaborazione da parte degli alunni coinvolti di un patto di comportamento sottoscritto dall'alunno dai genitori e dai docenti.

- 7) Segnalazione ai servizi sociali e/o forze di Polizia in accordo con il Dirigente scolastico.

MONITORAGGIO

Verbalizzare l'andamento degli interventi, dei nuovi episodi, etc.

- 1) Utilizzo di questionari per gli alunni coinvolti e degli spettatori passivi o gregari.
- 2) Osservazioni calendarizzate specialistiche e dei docenti.
- 3)** Incontro con le famiglie in varie fasi del percorso.

**SCHEDA PER L'INDIVIDUAZIONE/MONITORAGGIO DEI FATTI PRESUNTI O TALI
DI BULLISMO E CYBERBULLISMO**

Si ricorda che in caso di cyberbullismo occorre far rimuovere tempestivamente i materiali presenti in Rete o nelle chat di classe dagli Enti preposti. Contattare il Dirigente con urgenza.

NOME COORDINATORE _____ **CLASSE** _____ **ANNO SCOLASTICO** _____

DATA				
FATTI ACCERTATI				
FATTI PRESUNTI				

OPINIONI RACCOLTE				
PROVVEDIMENTI RIPARATORI O SANZIONATORI <i>(consultare il Regolamento di Istituto)</i>				
ALLEGATI <i>(verbali, copia note, osservazioni, convocazione famiglie...)</i>				

EVENTO SEGNALATO AL DIRIGENTE SCOLASTICO IN DATA				
FIRMA				