ISTITUTO COMPRENSIVO STATALE «C. EDERLE»
Corso Fraccaroli, 58 – 37049 Villa Bartolomea (VR)
C.M. VRIC84600R · C.F. 82000230233 · Tel. 0442 1833810
vric84600r@istruzione.it · vric84600r@pec.istruzione.it · www.icvillabartolomea.edu.it

DOCUMENTO DI ePOLICY · PROGETTO GENERAZIONI CONNESSE

ePolicy d'Istituto

IC Villa Bartolomea – aggiornamento a.s. 2026/2027

Prima approvazione: 25/09/2025 (piattaforma Generazioni Connesse)	**Approvazione:** Collegio dei Docenti, delibera n. 38 del 19/05/2025; Consiglio di Istituto, delibera n. 20/2025 del 30/06/2025
Sede: Corso Fraccaroli, 58 – 37049 Villa Bartolomea (VR)	**Documenti collegati:** Codice interno antibullismo, Protocollo per le emergenze, Regolamento d'Istituto, Patto di corresponsabilità

Che cosa cambia in questo aggiornamento

- adeguamento alla **L. 70/2024**, che ha modificato la L. 71/2017, e collegamento con il **Codice interno** antibullismo, il **Team** antibullismo e il **Tavolo permanente di monitoraggio**;
- eliminazione delle note-guida della piattaforma, dei riferimenti alla scuola secondaria di II grado, al «Municipio» e al Documento programmatico sulla sicurezza (abolito nel 2012);
- correzione dei riferimenti sull'obbligo di denuncia (art. 331 c.p.p.; art. 361 c.p.) e sulla segnalazione delle situazioni di pregiudizio (art. 9 L. 184/1983);
- regole sui dispositivi personali coerenti con il divieto di uso dello smartphone nel primo ciclo (nota MIM dell'11/07/2024);
- completamento del capitolo 4 con gli attori del territorio e gli allegati con le procedure.

Cap. 1	Presentazione dell'ePolicy: scopo; ruoli e responsabilità; integrazione con regolamenti e normativa; condivisione e comunicazione; piani di azione; risorse
Cap. 2	Sensibilizzazione e prevenzione: azioni; curricolo digitale; kit didattico
Cap. 3	Infrastruttura e strumentazione ICT: protezione dei dati; accesso a Internet; strumenti di comunicazione online (PUA); dispositivi personali
Cap. 4	Segnalazione e gestione dei casi: cosa segnalare; come segnalare, con quali strumenti e a chi; attori del territorio; allegati con le procedure

Capitolo 1 – Presentazione dell'ePolicy

1.1 Scopo dell'ePolicy

L'ePolicy ha come obiettivo principale promuovere le competenze digitali per un uso delle tecnologie positivo, critico e consapevole da parte delle alunne e degli alunni, guidati dagli adulti coinvolti nel processo educativo. La competenza digitale è una delle competenze chiave per l'apprendimento permanente (Raccomandazione del Consiglio dell'Unione europea del 22 maggio 2018) e permette a ogni cittadino di esercitare i propri diritti anche negli ambienti digitali (ONU, Commento generale n. 25 sui diritti dei minori in relazione all'ambiente digitale).

L'ePolicy è un documento programmatico che persegue quattro obiettivi:

- il piano di azioni triennale per promuovere nell'intera comunità scolastica l'uso sicuro, responsabile e positivo della rete;
- le misure di prevenzione e di sensibilizzazione sui comportamenti online a rischio;
- le norme di comportamento e le procedure di utilizzo delle tecnologie dell'informazione e della comunicazione (ICT) a scuola;
- le misure per la rilevazione, la segnalazione e la gestione delle situazioni a rischio legate a un uso scorretto delle tecnologie digitali.

1.2 Ruoli e responsabilità

Perché l'ePolicy sia uno strumento operativo efficace, ciascuno, secondo il proprio ruolo, si impegna ad attuarla e a promuoverla.

Il Dirigente scolastico

- promuove la cultura della sicurezza online, in linea con il quadro normativo e con le indicazioni del Ministero, e la inserisce nelle misure di sicurezza dell'Istituto;
- garantisce sistemi per un uso sicuro delle ICT e di Internet, con adeguati filtri di navigazione;
- è responsabile della gestione dei dati e della sicurezza delle informazioni, con il supporto del Responsabile della protezione dei dati;
- assicura a tutto il personale una formazione adeguata sulla sicurezza online;
- conosce e attua le procedure da seguire in caso di grave incidente di sicurezza online;
- valuta i rischi nell'uso degli strumenti digitali, in modo coerente con gli obiettivi educativi del PTOF, e garantisce un sistema di monitoraggio della sicurezza online con le figure di sistema;
- coordina il Team antibullismo e per l'emergenza e presiede il Tavolo permanente di monitoraggio previsto dal Codice interno.

L'animatore digitale e il Team per l'innovazione digitale

Sono corresponsabili, con il Referente per l'ePolicy, dell'attuazione dei piani di azione, in particolare per la formazione dei docenti, e del controllo dell'accesso degli alunni alle ICT.

Il Referente per il bullismo e il cyberbullismo

Designato dal Collegio dei Docenti ai sensi dell'art. 4, comma 3, della L. 71/2017, come modificata dalla L. 70/2024, coordina le iniziative di prevenzione e contrasto del bullismo e del cyberbullismo, riceve le segnalazioni, coordina il Team ed è corresponsabile, con il team ePolicy, dell'attuazione dei piani di azione.

Il Team antibullismo e per l'emergenza

In coerenza con le Linee di orientamento (D.M. n. 18 del 13/01/2021, trasmesse con nota prot. n. 482 del 18/02/2021) e con il Codice interno, il Team coadiuva il Dirigente scolastico, che lo coordina, nella definizione degli interventi di prevenzione e nella gestione dei casi; promuove la conoscenza dei fenomeni con progetti che coinvolgono genitori, alunni e personale; fa conoscere la propria esistenza come riferimento per segnalazioni e informazioni. Nelle situazioni acute interviene in composizione ristretta (Dirigente, Referente e, se necessario, esperti dei servizi del territorio). Promuove l'aggiornamento dell'ePolicy e monitora le segnalazioni.

Il Tavolo permanente di monitoraggio

Istituito ai sensi dell'art. 4, comma 2-bis, della L. 71/2017, con rappresentanti degli studenti della scuola secondaria di I grado, dei docenti, delle famiglie ed esperti di settore, monitora l'andamento dei fenomeni su dati aggregati, propone iniziative di prevenzione e verifica l'attuazione del Codice interno e dell'ePolicy.

I docenti

Hanno un ruolo centrale nel diffondere un uso responsabile delle ICT e della rete: integrano la propria disciplina con approfondimenti e promuovono l'uso delle tecnologie nella didattica; accompagnano gli alunni nelle attività con dispositivi connessi; li educano alla prudenza, a non fornire dati personali, ad abbandonare i siti con contenuti che turbano e a non incontrare persone conosciute in rete senza averne parlato con i genitori; informano sui rischi della rete senza demonizzarla. Osservano i comportamenti a rischio e hanno il dovere di segnalare subito al Dirigente e al Referente qualunque problema, violazione o abuso, anche online, che coinvolga gli alunni, per definire con il consiglio di classe strategie condivise.

Il Responsabile della protezione dei dati (RPD/DPO)

Conosce l'ePolicy, fornisce consulenza sugli obblighi del Regolamento (UE) 2016/679, sorveglia l'osservanza della normativa sulla protezione dei dati ed è corresponsabile delle azioni di informazione e formazione dell'Istituto in materia.

Il personale amministrativo, tecnico e ausiliario (ATA)

È coinvolto nelle pratiche di prevenzione, compresa l'attuazione dell'ePolicy, ed è tenuto a segnalare comportamenti non adeguati ed episodi di bullismo o cyberbullismo.

Le alunne e gli alunni

In relazione all'età e al grado di maturità, usano al meglio le tecnologie digitali secondo le indicazioni dei docenti; con il supporto della scuola imparano a tutelarsi online, a tutelare i compagni e a rispettarli; partecipano ai progetti sull'uso positivo della rete e diffondono quanto appreso, anche con la peer education. Nella scuola secondaria di I grado i loro rappresentanti partecipano al Tavolo permanente e sono coinvolti nella costruzione dei piani di azione.

I genitori e gli adulti di riferimento

In continuità con la scuola, partecipano alle attività di educazione all'uso consapevole delle tecnologie e dei dispositivi personali; si confrontano con i docenti sulle linee educative e comunicano i problemi rilevati; condividono quanto previsto dall'ePolicy e dal Patto di corresponsabilità. I loro rappresentanti partecipano alla definizione e all'attuazione dell'ePolicy e al Tavolo permanente.

Gli enti esterni e le associazioni

Gli enti pubblici e privati e le associazioni che realizzano iniziative nella scuola si conformano all'ePolicy, ne rispettano i requisiti di qualità, promuovono comportamenti sicuri durante le attività e adottano misure di tutela dei minori, per individuare e prendere in carico tempestivamente eventuali problemi.

1.3 Integrazione dell'ePolicy nei documenti scolastici

L'ePolicy è richiamata nel Regolamento d'Istituto, che contiene le norme di comportamento e le procedure di utilizzo delle ICT a scuola, e nel **Codice interno per la prevenzione e il contrasto del bullismo e del cyberbullismo**, di cui costituisce parte integrante per gli aspetti digitali. Il Patto educativo di corresponsabilità richiama l'impegno della scuola a organizzare iniziative di formazione e informazione per le famiglie e l'impegno delle famiglie a parteciparvi. Il PTOF contiene le azioni di educazione ai media legate all'ePolicy e il RAV ne monitora gli esiti nella priorità «Esiti in termini di benessere a scuola».

1.4 Condivisione e comunicazione dell'ePolicy

L'efficacia dell'ePolicy dipende dalla sua conoscenza nella comunità scolastica. Il documento è accompagnato da due versioni sintetiche, una per gli alunni e una per le famiglie, con un linguaggio adatto: la prima è usata nelle attività di educazione civica, la seconda è illustrata negli incontri con le famiglie. L'ePolicy è pubblicata sul sito della scuola e richiamata nel Patto di corresponsabilità.

Per il territorio la presenza dell'ePolicy è garanzia di un presidio attento al rapporto tra giovani, rete e tecnologie: l'Istituto è un luogo di confronto e di sperimentazione per istituzioni, imprese ed enti del Terzo settore che vogliono costruire progetti di cittadinanza digitale. L'adozione dell'ePolicy è comunicata all'Ufficio scolastico regionale e ai Comuni di Villa Bartolomea e Castagnaro (servizi istruzione e servizi sociali).

1.5 I piani di azione

I piani di azione sono il programma triennale con cui la scuola promuove la conoscenza delle regole e dei protocolli adottati: rilevazione dei bisogni, iniziative di informazione e formazione per docenti, alunni e famiglie, monitoraggio e valutazione delle azioni, anche nel RAV.

Anno	Azioni
1° anno – a.s. 2025/26	• presentazione dell'ePolicy ai docenti e alle famiglie (anche negli open day e nel Safer Internet Day) e diffusione delle versioni sintetiche; • rilevazione dei bisogni formativi dei docenti e degli interessi e comportamenti delle famiglie sull'uso del digitale; • avvio del kit didattico in alcune classi pilota; • integrazione dell'ePolicy nei documenti dell'Istituto; aggiornamento della PUA e delle regole sui dispositivi personali; • procedure di segnalazione anche in linguaggio adatto agli alunni; reportistica delle segnalazioni e degli esiti.
2° anno – a.s. 2026/27	• formazione dei docenti (almeno il 60%) sulla base della rilevazione, anche con il percorso di Generazioni Connesse e la piattaforma ELISA; • uso del kit didattico nei percorsi di educazione civica digitale; • rilevazione di interessi, bisogni e abitudini digitali degli alunni e rilevazione annuale del clima scolastico; • formazione per alunni e famiglie con i percorsi di Generazioni Connesse; • attuazione del Codice interno, del Protocollo e del Tavolo permanente; Giornata del rispetto (20 gennaio).
3° anno – a.s. 2027/28	• verifica degli esiti dei piani di azione e aggiornamento dell'ePolicy; • consolidamento della peer education nella scuola secondaria e diffusione delle buone pratiche.

1.6 Le risorse di Generazioni Connesse

Kit didattico; area formazione per docenti, famiglie e alunni; canali YouTube, Instagram, TikTok e Facebook con webinar e video per destinatari diversi; Helpline 1.96.96.

Capitolo 2 – Sensibilizzazione e prevenzione

2.1 Sensibilizzazione e prevenzione

La vita in rete di docenti, alunni e famiglie deve essere accompagnata dalla consapevolezza critica delle caratteristiche degli ambienti e dei servizi online e dalle competenze per viverli al meglio. L'ePolicy sviluppa azioni rivolte all'intera comunità scolastica per promuovere una cittadinanza digitale fatta di conoscenza dei diritti, dei rischi e delle opportunità della rete. Le iniziative di prevenzione del bullismo e del cyberbullismo sono indicate nel Codice interno (art. 11): educazione civica digitale, Giornata del rispetto, Safer Internet Day, peer education, incontri con le famiglie, formazione del personale, rilevazione del clima.

2.2 Il curricolo digitale

Il quadro europeo DigComp 2.2 offre la cornice per individuare temi e competenze da proporre, non solo agli alunni. Per gli alunni trova sviluppo nel curricolo di educazione civica (L. 92/2019; Linee guida adottate con D.M.

183/2024, nucleo «Cittadinanza digitale»). In ogni classe è previsto almeno un momento didattico specifico, adatto all'età, sui temi dell'ePolicy, anche con il kit didattico.

2.3 Il kit didattico

Il progetto Generazioni Connesse mette a disposizione di docenti e alunni, dalla scuola dell'infanzia alla secondaria, un kit con materiali per le lezioni e per l'aggiornamento su sicurezza in rete, etica e digitale, algoritmi e dati. Il kit può essere usato per intero o in parte, secondo le scelte del docente.

Capitolo 3 – Infrastruttura e strumentazione ICT

3.1 Protezione dei dati personali

La protezione dei dati personali è un diritto fondamentale (art. 8 della Carta dei diritti fondamentali dell'Unione europea; art. 16 TFUE). Le norme di riferimento sono il Regolamento (UE) 2016/679 (GDPR) e il D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali). L'Istituto ha designato il Responsabile della protezione dei dati (RPD/DPO), definisce l'organigramma privacy con le autorizzazioni del personale, rilascia le informative, tiene il registro dei trattamenti e, per le piattaforme digitali usate con gli alunni, nomina i fornitori responsabili del trattamento e valuta i rischi.

3.2 Accesso a Internet

L'accesso alla rete dell'Istituto avviene con credenziali personali e con sistemi di filtro dei contenuti; la rete per la didattica è separata da quella amministrativa. Gli alunni navigano solo sotto la guida del docente.

3.3 Strumenti di comunicazione online: la Politica d'uso accettabile (PUA)

La Politica d'uso accettabile e responsabile della rete (PUA) raccoglie le regole sull'uso della rete a scuola e a casa da parte degli alunni e di tutto il personale, compresi i professionisti esterni. Illustra vantaggi e rischi di Internet e vieta, tra l'altro, la ricerca di materiale non adatto, le azioni illecite, il gioco online con la rete scolastica, la violazione della riservatezza e del diritto d'autore, nel rispetto dei dati di ciascuno e in particolare degli alunni.

3.4 Strumentazione personale

In applicazione della nota MIM prot. n. 5274 dell'11/07/2024, nella scuola dell'infanzia, nella primaria e nella secondaria di I grado agli alunni è vietato l'uso del telefono cellulare durante l'orario scolastico, anche a fini educativi e didattici, salvo che sia previsto dal PEI o dal PDP o per documentate e oggettive condizioni personali. Tablet e computer, anche personali se autorizzati, si usano solo per attività didattiche e sotto la guida del docente. Sono vietate le riprese di persone senza autorizzazione e la loro diffusione. Le modalità di custodia dei dispositivi sono stabilite dal Regolamento d'Istituto.

Capitolo 4 – Segnalazione e gestione dei casi

4.1 Cosa segnalare

Il capitolo contiene le procedure per la segnalazione e la gestione dei problemi legati a comportamenti online a rischio. Sono una guida per il personale, per i professionisti e le organizzazioni esterne che operano con la scuola, e sono illustrate a genitori, alunni e personale con incontri, locandine, il sito e i collegi docenti. Le procedure di dettaglio sono nel Codice interno e nel Protocollo per la gestione delle emergenze (paragrafo 4.4).

Cyberbullismo. Occorre capire se si tratta davvero di cyberbullismo o di un altro problema, considerando il contesto e le modalità (c'è un pubblico? avviene tra coetanei? è ripetuto e intenzionale? c'è un danno percepito dalla vittima?) e valutare il disagio degli alunni coinvolti, anche per un eventuale supporto psicologico o di mediazione.

Adescamento online (grooming). Se si sospetta un caso, non si cancellano le prove dai dispositivi usati dal minore e non ci si sostituisce a lui nelle conversazioni con l'adescatore. È fondamentale valutare il benessere del minore e

il rischio che corre; la legge prevede che il minore vittima o testimone di questi reati sia ascoltato dalle autorità con l'ausilio di un esperto in psicologia o psichiatria infantile.

Sexting e diffusione di immagini intime. Se immagini o video, anche prodotti dagli stessi minori, sfuggono al loro controllo e vengono diffusi senza consenso, l'obiettivo è tutelare il minore e ottenere la rimozione del materiale e il blocco della sua diffusione. Il contenuto non va copiato, salvato né inoltrato: si informa subito il Dirigente, che si rivolge alla Polizia Postale.

Rimozione dei contenuti. Il minore ultraquattordicenne vittima di cyberbullismo, o chi esercita la responsabilità genitoriale, può chiedere al titolare del trattamento o al gestore del sito o del social network l'oscuramento, la rimozione o il blocco dei contenuti (art. 2 L. 71/2017). Se il gestore non comunica entro 24 ore di aver preso in carico la richiesta e non provvede entro 48 ore, ci si può rivolgere al Garante per la protezione dei dati personali, che provvede entro 48 ore.

Servizi utili: Helpline 1.96.96 e chat di Telefono Azzurro per supporto ed emergenze; «Clicca e segnala» di Telefono Azzurro e «STOP-IT» di Save the Children per segnalare materiale pedopornografico online.

4.2 Come segnalare: quali strumenti e a chi

L'insegnante, nell'esercizio delle sue funzioni, è un pubblico ufficiale (art. 357 c.p.): la funzione non si limita alle lezioni ma comprende tutte le attività educative, compresi gli incontri con i genitori (Cass. pen. n. 15367/2014). Le situazioni problematiche legate all'uso delle tecnologie sono gestite dal **Team antibullismo e per l'emergenza**, composto dal Dirigente, dal Referente per il bullismo e il cyberbullismo e dai docenti formati, con l'animatore digitale e, se necessario, con esperti esterni.

Caso A – Sospetto. Il docente sospetta che tra gli alunni stia accadendo qualcosa riconducibile a bullismo, cyberbullismo, sexting o adescamento: informa per iscritto il Referente e il Dirigente, riportando in modo dettagliato e oggettivo i dati e le informazioni (Scheda di prima segnalazione). Il Dirigente e il Team valutano il caso, anche in vista di una segnalazione alle autorità, e attivano gli interventi educativi.

Caso B – Evidenza. Il docente ha evidenza certa dei fatti: informa subito per iscritto il Referente e il Dirigente. Si procede alla valutazione approfondita e, se i fatti hanno rilevanza penale, il Dirigente presenta denuncia all'autorità giudiziaria.

Davanti a un fatto che può costituire reato procedibile d'ufficio l'insegnante non svolge indagini, ma ha l'obbligo di riferirlo senza ritardo, tramite il Dirigente, all'autorità giudiziaria (art. 331 c.p.p.); l'omissione è punita dall'art. 361 c.p. L'autorità competente è la **Procura della Repubblica presso il Tribunale per i minorenni** di Venezia se il presunto autore è minorenne, la **Procura della Repubblica presso il Tribunale ordinario** se è maggiorenne.

Le situazioni di **pregiudizio** – condizioni di rischio o di grave difficoltà che causano un danno reale o potenziale alla salute, allo sviluppo o alla dignità del minore – vanno segnalate alla Procura presso il Tribunale per i minorenni (art. 9 L. 184/1983) e ai servizi sociali. La segnalazione è il primo passo per aiutare il minore.

Valutando ogni situazione, si possono attivare colloqui individuali con tutti i minori coinvolti – vittime, testimoni, autori – e il coinvolgimento dei genitori, considerando l'impatto educativo e il contesto emotivo. Gli incontri di mediazione si valutano caso per caso, tenendo conto dello stato emotivo dei minori.

Anche i **genitori** possono e devono segnalare casi sospetti o evidenti al Dirigente, al coordinatore di classe, al Referente o al Team. Insegnanti, genitori e alunni possono rivolgersi alla Helpline 1.96.96, anche in chat, per supporto e consulenza.

Strumenti per gli alunni: colloquio con un docente o con il Referente; Scheda di prima segnalazione; indirizzo istituzionale del Referente; cassetta per le segnalazioni, anche anonime, nei plessi della secondaria. Le segnalazioni alimentano il monitoraggio, da cui partono azioni preventive, giornate di sensibilizzazione con gli enti del territorio e percorsi di peer education. Si rinvia al Codice interno, al Regolamento di disciplina, alle Linee di orientamento del 2021 e al Patto educativo di corresponsabilità.

4.3 Gli attori sul territorio

Soggetto	Quando rivolgersi
Servizi sociali dei Comuni di Villa Bartolomea e Castagnaro	Situazioni di disagio o di pregiudizio; famiglie che non collaborano; presa in carico del minore e della famiglia
Azienda ULSS 9 Scaligera (consultorio familiare, neuropsichiatria infantile)	Supporto psicologico e specialistico a vittime, autori e famiglie
Polizia Postale e per la sicurezza cibernetica (www.commissariatodips.it)	Contenuti illegali online, adescamento, diffusione di immagini intime, furti di identità; consulenza e incontri formativi
Arma dei Carabinieri e Polizia locale	Fatti di rilevanza penale; interventi urgenti; incontri sulla legalità
Procura della Repubblica presso il Tribunale per i minorenni di Venezia	Denunce per reati commessi da minorenni; segnalazioni di pregiudizio; misure rieducative
Garante per la protezione dei dati personali (cyberbullismo@gpdp.it)	Rimozione dei contenuti quando il gestore non provvede
Generazioni Connesse – Telefono Azzurro (1.96.96), Save the Children	Ascolto e consulenza; segnalazione di materiale pedopornografico («Clicca e segnala», «STOP-IT»)

4.4 Allegati con le procedure

- Codice interno per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo;
- Protocollo per la gestione delle situazioni di emergenza, con la Scheda di prima segnalazione (All. 1), la Scheda di valutazione approfondita (All. 2) e la Scheda di monitoraggio (All. 3);
- modello del Garante per la protezione dei dati personali per la segnalazione o il reclamo in materia di cyberbullismo;
- infografica «Bullismo e cyberbullismo: che cosa prevede la legge» per alunni e famiglie.

Villa Bartolomea, ____/____/2026

Il Dirigente scolastico
Avv. Giuliano Risi
(firmato digitalmente ai sensi del D.Lgs. 82/2005)

GIULIANO RISI
31.10.2026 13:41:53
GMT+01:00