

ALLEGATO F

E-POLICY E CODICE INTERNO PER LA PREVENZIONE E IL CONTRASTO DEI FENOMENI DI BULLISMO/CYBERBULLISMO

E-POLICY

Capitolo 1 — Presentazione dell'ePolicy

1.1 Scopo e funzione del documento

L'ePolicy è l'atto programmatico e organizzativo con cui il Liceo Classico Statale "Francesca Capece" di Maglie promuove, nell'intera comunità scolastica, la cittadinanza digitale e l'uso sicuro, responsabile, inclusivo e consapevole delle tecnologie dell'informazione e della comunicazione (ICT), in coerenza con la Raccomandazione del Consiglio dell'Unione Europea del 2018 sulle competenze chiave, il Commento Generale n. 25 del Comitato ONU sui diritti del fanciullo (2021) sui diritti dei minori negli ambienti digitali e il quadro europeo DigComp 3.3.

Essa non sostituisce il PTOF, il Regolamento d'Istituto, il Regolamento di disciplina, il Patto educativo di corresponsabilità, le informative privacy, il Piano per l'inclusione o i protocolli di emergenza, ma li coordina e vi rinvia. In caso di contrasto, prevalgono la legge, i regolamenti ministeriali vigenti, gli atti dell'autorità giudiziaria e le disposizioni formalmente adottate dagli organi competenti.

La presente ePolicy persegue quattro obiettivi: (1) pianificazione triennale di azioni per promuovere l'uso sicuro, responsabile e positivo della rete; (2) misure di prevenzione e sensibilizzazione sui comportamenti online a rischio; (3) norme comportamentali e procedure di utilizzo delle ICT in ambiente scolastico; (4) misure per la rilevazione, la segnalazione e la gestione delle situazioni rischiose.

L'ePolicy si applica alle attività scolastiche in presenza e a distanza, alle reti e piattaforme dell'Istituto, ai dispositivi personali utilizzati per finalità didattiche e alle attività esterne organizzate o autorizzate dalla scuola, senza estendere automaticamente la responsabilità dell'Istituto a ogni condotta privata estranea alle attività scolastiche. L'ePolicy è riesaminata almeno annualmente e comunque ogni volta che intervengano modifiche normative, organizzative, tecnologiche o significativi incidenti di sicurezza.

1.2 Quadro normativo di riferimento

Il documento è attuato alla luce della normativa vigente, tra cui:

- Legge 29 maggio 2017, n. 71 e successive modificazioni — Disposizioni a tutela dei minori per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo, come modificata dalla Legge 17 maggio 2024, n. 70 (art. 1 L. 70/2024);
- Legge 20 agosto 2019, n. 92 — insegnamento trasversale dell'educazione civica, con riferimento alla cittadinanza digitale e alla Consulta dei diritti e dei doveri del bambino e dell'adolescente digitale;
- Linee di orientamento per la prevenzione e il contrasto del bullismo e del cyberbullismo (D.M. 13 gennaio 2021, n. 18, e aggiornamenti), recanti anche l'indicazione delle procedure (art. 4 L. 71/2017);
- D.P.R. 24 giugno 1998, n. 249 — Statuto delle studentesse e degli studenti, in corso di adeguamento ai principi dell'art. 5 L. 70/2024 (emersione degli episodi di bullismo e cyberbullismo, integrazione del Patto educativo di corresponsabilità);

- Regio Decreto-Legge 20 luglio 1934, n. 1404, come modificato dall'art. 2 L. 70/2024 — misure rieducative del tribunale per i minorenni (progetto di intervento educativo con finalità rieducativa e riparativa);
- Regolamento (UE) 2016/679 (GDPR) e D.Lgs. 30 giugno 2003, n. 196, come modificato dal D.Lgs. 10 agosto 2018, n. 101;
- Codice penale e codice di procedura penale, con particolare riguardo alla qualifica di pubblico ufficiale (art. 357 c.p.), all'obbligo di denuncia (art. 331 c.p.p. e art. 361 c.p.), alla tutela rafforzata dei minori (art. 609-decies c.p.) e all'oltraggio a pubblico ufficiale (art. 341-bis c.p.);
- Legge 4 maggio 1983, n. 184 — obbligo di segnalazione al procuratore della Repubblica presso il tribunale per i minorenni dei minori in situazione di abbandono (art. 9) e relativa sanzione (art. 70);
- Codice civile — interventi a tutela dei minori (artt. 330, 333 e 403 c.c.) e responsabilità dei precettori (art. 2048, comma 2, c.c.);
- Convenzione ONU sui diritti del fanciullo (New York, 20 novembre 1989), ratificata e resa esecutiva con la Legge 27 maggio 1991, n. 176;
- Piano Nazionale Scuola Digitale (PNSD), di cui alla L. 13 luglio 2015, n. 107.

I riferimenti sono aggiornati dal responsabile del riesame. Non sono utilizzate formule che attribuiscono automaticamente a un singolo docente la responsabilità di qualificare penalmente un fatto o di decidere l'autorità competente: la scuola attiva tempestivamente i soggetti istituzionalmente competenti, senza svolgere indagini autonome.

1.3 Ruoli e responsabilità

Il Dirigente Scolastico

- promuove la cultura della sicurezza online e la integra nelle misure di sicurezza generali dell'Istituto;
- garantisce sistemi per un uso sicuro delle ICT, della rete internet e dei relativi ambienti, mediante adeguati sistemi informatici e di filtraggio, proporzionati, documentati e compatibili con privacy, inclusione e finalità didattiche;
- risponde della gestione dei dati e della sicurezza delle informazioni e garantisce al personale una formazione adeguata sulla sicurezza online;
- conosce e attua le procedure per gli incidenti di sicurezza online e assicura adeguate valutazioni di rischio;
- ove venga a conoscenza di atti di bullismo o cyberbullismo che coinvolgano studenti dell'Istituto, applica le procedure delle linee di orientamento, informa tempestivamente i genitori dei minori coinvolti, promuove iniziative educative anche con percorsi di mediazione scolastica e, nei casi più gravi o quando le iniziative educative non abbiano prodotto esito positivo, riferisce alle autorità competenti anche per l'eventuale attivazione delle misure rieducative di cui all'art. 25 del R.D.L. 1404/1934, come riformato dall'art. 2 L. 70/2024, salvo che il fatto costituisca reato (art. 5 L. 71/2017).

L'Animatore Digitale e il Team per l'Innovazione Digitale

- sono co-responsabili, con il Referente ePolicy, dell'attuazione dei piani di azione, con particolare riferimento alla formazione dei docenti;
- supportano tecnicamente e metodologicamente l'uso delle tecnologie negli spazi del Liceo e collaborano al controllo dell'accesso alle TIC, nel rispetto della normativa privacy e dello Statuto delle studentesse e degli studenti.

Il Referente per il Bullismo e il Cyberbullismo

- coordina le iniziative di prevenzione e contrasto del bullismo e del cyberbullismo (art. 4, comma 3, L. 71/2017);
- riceve le segnalazioni e le inoltra, secondo le procedure del Capitolo 4, al Dirigente Scolastico e al Team per l'emergenza. Non svolge attività investigativa né sostituisce l'autorità giudiziaria, i servizi sociali o le forze dell'ordine.

Il Team Antibullismo e per l'Emergenza

- è costituito con atto formale dell'Istituto, che ne indica componenti, sostituti, durata e contatti; coadiuva il Dirigente Scolastico — che lo presiede — nella definizione degli interventi di prevenzione e nella gestione dei casi, secondo le Linee di orientamento e la L. 71/2017 come modificata dalla L. 70/2024;
- interviene come gruppo ristretto (Dirigente, Referente, psicologo o pedagogo ove presente) nelle situazioni acute; opera secondo necessità e secondo il principio di riservatezza;
- promuove la redazione e l'applicazione dell'ePolicy e del codice interno, monitora le segnalazioni e redige la reportistica. Le funzioni preventive possono coinvolgere rappresentanti di studenti e genitori; la gestione dei casi individuali avviene soltanto con soggetti competenti e secondo il criterio di stretta necessità.

I Docenti

- integrano la propria disciplina con i temi della cittadinanza digitale e promuovono l'uso delle tecnologie nella didattica, educando gli studenti alla prudenza e alla protezione dei dati personali;
- osservano regolarmente i comportamenti a rischio e hanno il dovere di segnalare tempestivamente al Dirigente Scolastico, al Referente e al Consiglio di Classe qualunque problematica, violazione o abuso — anche online — che veda coinvolti studenti, senza diffondere informazioni non necessarie. In presenza di un rischio attuale o di una possibile notizia di reato, trasmettono immediatamente una comunicazione oggettiva al Dirigente e seguono le istruzioni ricevute; non interrogano informalmente i minori in modo suggestivo, non contattano il presunto autore online e non inoltrano immagini o materiale illecito.

Il Responsabile della Protezione dei Dati (RPD/DPO)

- informa, consiglia e sorveglia l'osservanza della normativa privacy, nei limiti degli artt. 37-39 GDPR, e funge da punto di contatto con gli interessati e con il Garante. Non è titolare del trattamento, non autorizza i trattamenti in luogo dell'Istituto e non è co-responsabile degli stessi per il solo fatto di fornire consulenza.

Il Personale Amministrativo, Tecnico e Ausiliario (ATA)

- è coinvolto nelle pratiche di prevenzione e nell'implementazione dell'ePolicy e segnala tempestivamente comportamenti non adeguati o episodi di bullismo/cyberbullismo rilevati negli spazi comuni o nei laboratori.

Le Studentesse e gli Studenti

- utilizzano le tecnologie digitali in coerenza con quanto richiesto dai docenti e con il proprio grado di maturità, rispettando persone, dati, dispositivi e regole di rete;
- partecipano attivamente ai progetti sull'uso positivo delle TIC, anche attraverso percorsi di peer education, e possono segnalare in forma riservata; contribuiscono, tramite i propri rappresentanti, alla condivisione dell'ePolicy e partecipano al tavolo permanente di monitoraggio.

I Genitori e gli Adulti di Riferimento

- condividono con la scuola la responsabilità educativa sottoscrivendo il Patto educativo di corresponsabilità e collaborano senza sostituirsi ai soggetti istituzionali;
- partecipano ai momenti formativi e segnalano eventuali criticità, collaborando per consentire l'emersione degli episodi di bullismo e cyberbullismo, secondo quanto previsto dall'art. 5 L. 70/2024.

Gli Enti Esterni Pubblici e Privati e le Associazioni

- si conformano alla politica della scuola per le iniziative rivolte ai più giovani, sottoscrivono le regole di comportamento, ricevono le istruzioni privacy e, quando trattano dati per conto della scuola, operano sulla base di un incarico o contratto conforme al GDPR.

1.4 Codice interno e tavolo permanente di monitoraggio

In attuazione dell'art. 4, comma 2-bis, L. 71/2017 (come introdotto dall'art. 1 L. 70/2024), il Liceo:

- adotta un codice interno per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo, predisposto come documento separato, parte integrante della presente ePolicy, pubblicato sul sito istituzionale e affisso negli spazi scolastici;
- istituisce un tavolo permanente di monitoraggio, del quale fanno parte rappresentanti degli studenti, degli insegnanti, delle famiglie ed esperti di settore (psicologo o pedagogo ove disponibile, referenti degli enti locali e delle associazioni territoriali), con i compiti di monitorare le segnalazioni e i relativi esiti, verificare l'efficacia delle azioni di prevenzione, proporre aggiornamenti del codice interno e dell'ePolicy e promuovere la cultura del rispetto.

Il codice interno e le linee di orientamento sono **recepiti nel regolamento d'istituto, anche con riferimento alle procedure da adottare** per la prevenzione e il contrasto del bullismo e del cyberbullismo (art. 4, comma 3, L. 71/2017); il regolamento e il Patto educativo di corresponsabilità sono integrati con specifici riferimenti alle condotte di bullismo e cyberbullismo e alle relative sanzioni disciplinari commisurate alla gravità degli atti compiuti (art. 5, comma 2, L. 71/2017).

1.5 Integrazione nei documenti scolastici

- Piano Triennale dell'Offerta Formativa (PTOF): accoglie le linee d'azione e la progettualità legata alla cittadinanza digitale, con obiettivi, attività, risorse e indicatori;
- Regolamento d'Istituto e Regolamento di disciplina: recepiscono le linee di orientamento e le procedure e indicano condotte, sanzioni e misure educative in modo tassativo o sufficientemente determinato, graduale e proporzionato;
- Patto educativo di corresponsabilità: richiama l'ePolicy e il codice interno e descrive gli impegni reciproci, senza trasformare la famiglia in garante assoluta di ogni condotta privata del minore;
- Rapporto di Autovalutazione (RAV) e Piano di Miglioramento: monitorano l'impatto delle azioni di prevenzione utilizzando dati aggregati, evitando la re-identificazione dei casi.

1.6 Condivisione e comunicazione

Il documento è: pubblicato in modo permanente sul portale web d'Istituto in sezione dedicata; accompagnato da versioni sintetiche (friendly) per studenti, famiglie e personale, che non possono modificare il contenuto giuridico della versione integrale; notificato tramite registro elettronico e circolari all'inizio di ogni anno scolastico; presentato negli incontri di accoglienza dei nuovi iscritti e delle famiglie, negli Open Day e nel Safer Internet Day; esaminato dal Collegio dei Docenti e dai Consigli di Classe e discusso con il Comitato dei Genitori e le rappresentanze degli studenti; comunicato all'Ufficio Scolastico Regionale e al Comune (servizi istruzione e sociali), nonché agli enti e alle associazioni che realizzano iniziative sui temi dell'educazione civica digitale.

1.7 I Piani di Azione

I piani di azione costituiscono il programma triennale di obiettivi e comprendono: rilevazione dei bisogni, iniziative informative e formative, formazione di docenti, studenti e famiglie, monitoraggio e valutazione (anche nell'ambito del RAV).

1° Anno di attuazione

- Modulo I — Sensibilizzazione e diffusione: presentazione dell'ePolicy ai docenti; diffusione alle famiglie e agli studenti (Open Day, Safer Internet Day); distribuzione delle versioni friendly; adozione del codice interno e insediamento del tavolo permanente di monitoraggio.
- Modulo II — Analisi dei bisogni e sperimentazione: rilevazione del fabbisogno formativo dei docenti; rilevazione di interessi, bisogni e comportamenti delle famiglie; avvio del kit didattico in classi pilota.
- Modulo III — Adeguamento normativo e documentale: integrazione dell'ePolicy e del codice interno nel PTOF, nel Regolamento e nel Patto di corresponsabilità; aggiornamento della PUA e della disciplina BYOD.
- Modulo IV — Procedure di rilevazione e gestione: definizione e pubblicazione delle procedure di segnalazione con linguaggio youth friendly; reportistica riservata delle segnalazioni.

2° Anno di attuazione

- Modulo I — Formazione del personale docente: formazione sulla cittadinanza digitale e prevenzione dei rischi online, con l'obiettivo di coinvolgere almeno il 60% del corpo docente.
- Modulo II — Estensione didattica e formazione allargata: adozione sistematica del kit didattico; rilevazione di interessi, bisogni e comportamenti degli studenti; formazione di studenti e famiglie; attivazione di percorsi di peer education.

3° Anno di attuazione

- Modulo I — Consolidamento: consolidamento del curriculum verticale di cittadinanza digitale allineato al DigComp 3.3; verifica dell'efficacia delle azioni nel RAV.
- Modulo II — Revisione: revisione dell'ePolicy, del codice interno e delle procedure alla luce dei dati di monitoraggio e delle novità normative; programmazione del triennio successivo.

In ogni anno, nella settimana che precede il **20 gennaio**, il Liceo riserva spazi ad attività didattiche in occasione della «**Giornata del rispetto**» istituita dall'art. 4 L. 70/2024, e partecipa al Safer Internet Day e alla Giornata nazionale contro il bullismo e il cyberbullismo (7 febbraio). Gli obiettivi quantitativi sono indicati nel PTOF o nel Piano di miglioramento solo dopo aver verificato risorse e disponibilità organizzativa.

Capitolo 2 — Sensibilizzazione e prevenzione

2.1 Le azioni di sensibilizzazione

La quotidianità in rete di docenti, studenti e famiglie deve essere caratterizzata da una consapevolezza critica degli ambienti e dei servizi online. In attuazione della L. 92/2019 e del quadro strategico di Generazioni Connesse, il Liceo sviluppa un percorso formativo continuo per l'intera comunità educante.

Obiettivi a breve termine (1° anno): somministrazione di questionari anonimi a studenti, docenti e famiglie; incontri e workshop in occasione del Safer Internet Day, della Giornata del rispetto (20 gennaio) e della Giornata nazionale contro il bullismo e il cyberbullismo (7 febbraio); diffusione delle versioni sintetiche dell'ePolicy e pubblicazione del glossario dei rischi online; adozione pilota del kit didattico nelle classi di snodo.

Obiettivi a lungo termine (triennio): consolidamento del curriculum verticale di cittadinanza digitale allineato al DigComp 3.3; formazione e aggiornamento di almeno il 60% del personale docente; strutturazione di percorsi di peer education; promozione della genitorialità digitale (tempo-schermo, privacy, benessere psicofisico).

2.2 Il Curriculum Digitale

Il Liceo struttura il curriculum digitale nell'ambito dell'insegnamento trasversale dell'educazione civica (L. 92/2019), assumendo il quadro DigComp 3.3 come riferimento. L'ePolicy e il codice interno costituiscono la linea guida pedagogica e operativa attorno a cui si sviluppano le unità di apprendimento.

L'implementazione si caratterizza per: **pianificazione trasversale e verticale**, con moduli graduati per età sulle cinque aree del DigComp 3.3 (alfabetizzazione su dati e informazioni; comunicazione e collaborazione; creazione di contenuti digitali; sicurezza; risoluzione dei problemi e benessere digitale); **unità didattiche annuali obbligatorie** in ciascuna classe, incentrate su diritti e doveri online, verifica delle fonti, protezione dei dati, diritto d'autore, identità digitale, gestione dei conflitti, cyberbullismo, diffusione non consensuale di immagini e ricorso ai canali di aiuto; **utilizzo del kit didattico di Generazioni Connesse**; **sinergia con i percorsi per famiglie e personale**. Le attività non devono esporre pubblicamente studenti coinvolti in casi reali e non devono utilizzare materiale lesivo non indispensabile. La peer education è svolta da studenti formati e sotto supervisione adulta; non comporta ascolto clinico, raccolta autonoma di dati o gestione di emergenze.

2.3 Il Kit Didattico

Il Liceo adotta il Kit Didattico di Generazioni Connesse quale strumento metodologico e operativo per tradurre i principi dell'ePolicy in percorsi d'aula concreti, anche sulle tematiche complesse della cittadinanza digitale (etica delle tecnologie, algoritmi, profilazione, datafication, intelligenza artificiale). Il suo utilizzo si organizza secondo: **flessibilità e adattabilità didattica** (selezione modulare delle schede in base alla maturità degli alunni); **strumento attivatore per l'educazione civica** (discussione guidata, pensiero critico, lavoro di gruppo, simulazioni); **aggiornamento e supporto al corpo docente**; **integrazione con la valutazione delle competenze** di cittadinanza e del comportamento.

Capitolo 3 — Gestione dell'infrastruttura e della strumentazione ICT

3.1 Protezione dei dati personali e GDPR

La protezione dei dati personali costituisce un diritto fondamentale (art. 8 della Carta dei diritti fondamentali dell'UE; art. 16 TFUE). Il Liceo tratta dati personali soltanto per finalità determinate e su una base giuridica individuata, nel rispetto del GDPR e del D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018.

Nomina del Responsabile della Protezione dei Dati (RPD/DPO): l'Istituto ha designato il proprio DPO, obbligatorio per gli organismi pubblici ai sensi dell'art. 37 GDPR; i contatti sono pubblicati sul sito istituzionale.

Organigramma privacy e designazione del personale: il Dirigente Scolastico, quale legale rappresentante del Titolare, autorizza e formalizza le istruzioni operative per il personale docente e ATA, individuando ruoli e responsabilità nell'accesso e nella gestione dei dati.

Base giuridica e informative: il trattamento per finalità istituzionali è fondato sull'art. 6, par. 1, lett. e), GDPR (esecuzione di un compito di interesse pubblico), con la disciplina di cui all'art. 2-ter D.Lgs. 196/2003: la comunicazione tra titolari e la diffusione dei dati sono ammesse solo se previste da una norma di legge o di regolamento. Le informative sono rese prima della raccolta e indicano titolare, contatti del DPO, finalità, categorie di dati, base giuridica, destinatari, tempi di conservazione, diritti e modalità di reclamo. **La scuola non richiede un consenso quando il trattamento trova la propria base in un obbligo legale o in un compito di interesse pubblico;** il consenso è utilizzato solo quando appropriato, separato per finalità e liberamente revocabile. La pubblicazione di immagini o video su sito e social è distinta dalla registrazione didattica interna.

Consenso dei minori: in attuazione dell'art. 8, par. 1, GDPR, il minore che ha compiuto i **quattordici anni** può esprimere autonomamente il consenso per i servizi della società dell'informazione; per i minori di età inferiore il consenso è prestato o autorizzato da chi esercita la responsabilità genitoriale, con informazioni rese in linguaggio chiaro e semplice (art. 2-quinquies D.Lgs. 196/2003).

Categorie particolari di dati: il trattamento di dati sulla salute o di vulnerabilità (es. DSA) è ammesso per motivi di interesse pubblico rilevante, ivi inclusi l'istruzione e la formazione in ambito scolastico (art. 2-sexies D.Lgs. 196/2003), nel rispetto di minimizzazione e proporzionalità.

Dati relativi agli studenti: su richiesta degli interessati, l'Istituto può comunicare o diffondere dati relativi agli esiti formativi per agevolare orientamento, formazione e inserimento professionale (art. 96 D.Lgs. 196/2003), ferma la tutela della riservatezza dello studente.

Registro dei trattamenti, misure di sicurezza e data breach: l'Istituto predispone e aggiorna il registro delle attività di trattamento e applica misure di sicurezza adeguate ai sensi dell'art. 32 GDPR. Il Documento programmatico sulla sicurezza (DPS) previsto dal previgente art. 34 D.Lgs. 196/2003 è stato abrogato dal D.Lgs. 101/2018 e non costituisce più riferimento. Sono adottate procedure per la gestione delle violazioni dei dati (data breach), con notifica al Garante e comunicazione agli interessati nei casi e nei termini previsti dagli artt. 33 e 34 GDPR.

Trattamento dei dati nelle procedure di segnalazione: per segnalazioni, questionari e monitoraggio si applicano i seguenti criteri minimi: accesso alle segnalazioni limitato al Dirigente e ai componenti autorizzati, con registrazione del protocollo e conservazione secondo il piano

documentale; questionari preferibilmente anonimi, con risultati solo aggregati; box fisico con apertura da almeno due soggetti autorizzati e verbale essenziale; e-mail dedicata su casella istituzionale con autenticazione forte e deleghe formalizzate; evidenze digitali conservate integralmente con accesso ristretto e nessun inoltro a soggetti non autorizzati; reportistica con soli dati aggregati e non re-identificativi.

3.2 La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.)

La P.U.A. definisce le regole di accesso e utilizzo della rete scolastica, delle piattaforme online e dei servizi cloud da parte di studenti, docenti, personale ATA, collaboratori ed esperti esterni.

Infrastruttura, accesso e credenziali: l'accesso a rete, registro elettronico, posta e piattaforme avviene esclusivamente tramite credenziali personali e riservate, non cedibili a terzi; l'Istituto adotta sistemi di filtraggio dei contenuti, firewall e monitoraggio per finalità di sicurezza e funzionamento. Eventuali filtri, log o controlli tecnici sono adottati **secondo necessità, proporzionalità e informativa**: non è previsto un monitoraggio generalizzato e indiscriminato dei contenuti personali degli studenti.

Comportamenti consentiti e promossi: uso delle tecnologie strettamente finalizzato ad attività didattiche, educative, di ricerca e di gestione amministrativa; rispetto della netiquette; protezione dei dati di accesso; linguaggio corretto e decoroso in tutti gli ambienti digitali d'Istituto.

Comportamenti vietati: consultare, scaricare, conservare o diffondere materiale pornografico, violento, discriminatorio o illegale; utilizzare la rete per gioco d'azzardo, gaming non autorizzato, attività commerciali o download illegale; violare la riservatezza altrui mediante registrazione, pubblicazione o condivisione non autorizzata di immagini, audio, video o dati personali; svolgere attività di hacking, alterazione delle configurazioni di rete, introduzione di malware o furto d'identità.

Misure e sanzioni: in caso di rischio tecnico immediato l'Istituto può sospendere temporaneamente un account o isolare un dispositivo per contenere l'incidente; tale misura tecnica non costituisce automaticamente sanzione disciplinare. Le sanzioni sono applicate esclusivamente secondo il Regolamento di disciplina, con contestazione, valutazione individuale, proporzionalità, possibilità di difesa e competenza dell'organo previsto, fatto salvo il ricorso alle autorità competenti nei casi di potenziale illecito civile o penale.

3.3 Dispositivi personali (BYOD)

I dispositivi personali (smartphone, tablet, e-reader, notebook) sono utilizzabili soltanto su indicazione del docente e per finalità didattiche, di ricerca o di inclusione (in particolare per alunni con DSA/BES); in assenza di autorizzazione devono essere spenti o riposti secondo il Regolamento d'Istituto.

La custodia, l'integrità e il corretto funzionamento del dispositivo restano sotto la responsabilità esclusiva dell'alunno e della sua famiglia: **la scuola non assume un obbligo generale di custodia dei dispositivi personali**, salvo che il dispositivo sia stato consegnato o depositato secondo specifiche disposizioni dell'Istituto, ferma restando la disciplina degli obblighi di vigilanza concretamente applicabili. Durante l'orario scolastico il collegamento avviene prioritariamente tramite la rete Wi-Fi protetta d'Istituto.

Ogni attività BYOD deve prevedere un'alternativa per chi non possiede un dispositivo o necessita di strumenti compensativi: qualora un alunno non disponga di un dispositivo, l'Istituto fornisce in comodato o in uso d'aula una dotazione tecnologica. L'uso didattico non autorizza la pubblicazione o diffusione di immagini, audio, video o dati personali: registrazioni e immagini sono vietate salvo specifica finalità, istruzione del docente, informativa e base giuridica applicabile; la pubblicazione richiede una valutazione ulteriore e, ove necessario, consenso separato dell'esercente la responsabilità genitoriale. L'uso non autorizzato dei dispositivi per motivi personali durante le lezioni è sanzionato secondo il Regolamento di disciplina.

Capitolo 4 — Segnalazione e gestione dei casi

4.1 Cosa segnalare

Le procedure del presente capitolo costituiscono la guida costante per il personale della scuola nell'identificazione di una situazione a rischio, nella presa in carico e nell'individuazione dell'intervento migliore. Le principali fattispecie oggetto di rilevazione sono:

Bullismo: l'art. 1, comma 1-bis, L. 71/2017 definisce il bullismo come "l'aggressione o la molestia reiterate, da parte di una singola persona o di un gruppo di persone, in danno di un minore o di un gruppo di minori, idonee a provocare sentimenti di ansia, di timore, di isolamento o di emarginazione, attraverso atti o comportamenti vessatori, pressioni o violenze fisiche o psicologiche, istigazione al suicidio o all'autolesionismo, minacce o ricatti, furti o danneggiamenti, offese o derisioni". Rilevano la reiterazione della condotta e l'idoneità lesiva, anche in forma non telematica.

Cyberbullismo: l'art. 1, comma 2, L. 71/2017 definisce il cyberbullismo come 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 online aventi ad oggetto anche uno o più componenti della famiglia del minore, il cui scopo intenzionale e predominante sia isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso o la loro messa in ridicolo. Nell'accertamento vanno considerati contesto, presenza di un "pubblico" virtuale, reiterazione, intenzionalità e danno percepito dalla vittima.

Adescamento online (grooming): in caso di sospetto di avvicinamento manipolatorio di un minore da parte di un adulto in rete, il personale non deve cancellare le prove digitali, non deve sostituirsi al minore rispondendo all'adescatore e deve attivare tempestivamente le forze dell'ordine e i servizi specialistici. Per alcune tipologie di reati, ivi incluso il grooming, la persona minorenni coinvolta in qualità di vittima o testimone deve essere ascoltata con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Sexting e diffusione non consenziente di contenuti intimi: l'obiettivo primario è la tutela della dignità del minore, la prevenzione della catena di condivisione tra pari e l'assistenza nelle procedure di blocco e rimozione. La diffusione non consensuale di immagini o video a contenuto sessualmente esplicito può integrare il delitto di cui all'art. 612-ter c.p., per il quale l'art. 7 L. 71/2017 prevede — fino a quando non sia proposta querela o presentata denuncia — la procedura di **ammonimento** da parte del questore, applicabile anche ai reati commessi mediante la rete internet da minorenni di età superiore ai quattordici anni nei confronti di altro minorenne, con sanzione amministrativa pecuniaria a carico di chi esercita la responsabilità genitoriale in caso di recidiva successiva all'ammonimento.

Oscuramento dei contenuti e servizi di supporto: in applicazione dell'art. 2 L. 71/2017, ciascun minore ultraquattordicenne, nonché ciascun genitore o soggetto esercente la responsabilità del minore che abbia subito atti 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. L'Istituto promuove l'utilizzo dei servizi nazionali di supporto: Helpline 19696 e chat di Telefono Azzurro, numero di pubblica utilità **«Emergenza infanzia 114»** (oggetto di potenziamento ai sensi dell'art. 3 L. 70/2024), portali "STOP-IT" di Save the Children e "Clicca e segnala" di Telefono Azzurro, Polizia Postale e delle Comunicazioni.

4.2 Qualifica giuridica del personale e obblighi di segnalazione

Il docente e il dirigente scolastico come pubblici ufficiali: il docente riveste la qualifica di **pubblico ufficiale** ai sensi dell'art. 357 c.p. nell'esercizio di tutte le sue funzioni educative e di vigilanza: l'esercizio delle funzioni dell'insegnante non è circoscritto alla tenuta delle lezioni, ma si estende alle connesse attività preparatorie, contestuali e successive, ivi compresi gli incontri con i genitori degli allievi (Cass. pen., Sez. V, n. 15367/2014). La medesima qualifica è riconosciuta al dirigente scolastico, legittimato a manifestare all'esterno la volontà provvedimentoale

dell'amministrazione scolastica, a esercitare il potere disciplinare, a rilasciare titoli scolastici e a rappresentare l'istituto nei rapporti contrattuali (Cass. pen., Sez. III, n. 37105/2023).

L'obbligo di denuncia: i pubblici ufficiali e gli incaricati di un pubblico servizio che hanno notizia di un reato perseguibile d'ufficio **devono farne denuncia per iscritto, senza ritardo**, al pubblico ministero o a un ufficiale di polizia giudiziaria, anche quando non sia individuata la persona alla quale il reato è attribuito (art. 331 c.p.p.). La mancata o ritardata denuncia integra il delitto di **omessa denuncia di reato** di cui all'art. 361 c.p., come confermato anche con riferimento a fatti commessi da studenti in contesti scolastici (Cass. pen., Sez. V, n. 24572/2021).

Il presupposto dell'obbligo è la **notizia di reato**: un'informazione in grado di richiamare la commissione di un reato, ossia un fatto corrispondente a una fattispecie incriminatrice. Il **mero sospetto** di una possibile attività illecita non fa sorgere l'obbligo, che sorge quando il pubblico ufficiale è in grado di individuare gli elementi costitutivi del reato perseguibile d'ufficio (Cass. pen., Sez. VI, n. 35960/2017; Cass. pen., Sez. V, n. 26081/2008). La mera omissione dell'attività ispettiva o istruttoria preliminare non si identifica con l'omessa denuncia (Cass. pen., Sez. VI, n. 27715/2019). In presenza di una notizia di reato, il personale non deve svolgere indagini autonome ma riferire quanto appreso, conservando gli elementi di riscontro.

La segnalazione delle situazioni di pregiudizio: con riguardo alle situazioni di abbandono, i pubblici ufficiali, gli incaricati di un pubblico servizio e gli esercenti un servizio di pubblica necessità **devono riferire al più presto al procuratore della Repubblica presso il tribunale per i minorenni** sulle condizioni di ogni minore in situazione di abbandono di cui vengano a conoscenza in ragione del proprio ufficio (art. 9 L. 184/1983); la mancata segnalazione è punita ai sensi dell'art. 328 c.p. (art. 70 L. 184/1983). Quando il minore è esposto, nell'ambiente familiare, a grave pregiudizio e pericolo per la sua incolumità psico-fisica, la pubblica autorità interviene ai sensi dell'art. 403 c.c.. Le situazioni di pregiudizio che non configurano abbandono sono segnalate ai servizi sociali e al tribunale per i minorenni, che può adottare provvedimenti limitativi o ablativi della responsabilità genitoriale ai sensi degli artt. 330 e 333 c.c. L'art. 609-decies c.p. prevede inoltre la comunicazione al tribunale per i minorenni quando si procede per determinati delitti commessi in danno di minorenni. La Convenzione ONU sui diritti del fanciullo, ratificata con la L. 176/1991, sancisce all'art. 3 il principio dell'interesse superiore del minore come considerazione preminente (Cass. civ., Sez. I, n. 23669/2023).

Autorità competenti: Procura della Repubblica presso il tribunale per i minorenni (presunto autore minorenne; situazioni di pregiudizio o abbandono); Procura della Repubblica ordinaria (vittima minorenne e presunto autore maggiorenne); Polizia Postale e delle Comunicazioni (reati commessi mediante la rete). Il personale non attribuisce a sé compiti investigativi e non ritarda le comunicazioni dovute in attesa di completare accertamenti interni.

4.3 Procedura di oscuramento, rimozione o blocco dei contenuti

In applicazione dell'art. 2 L. 71/2017:

- il minore ultraquattordicenne, ovvero ciascun genitore o soggetto esercente la responsabilità del minore che abbia subito atti di cyberbullismo, inoltra 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, previa conservazione dei dati originali e con identificazione espressa dei contenuti tramite URL, anche qualora le condotte non integrino fattispecie penali;
- entro ventiquattro ore dal ricevimento dell'istanza, il soggetto responsabile deve comunicare di avere assunto l'incarico di provvedere; entro quarantotto ore deve avervi provveduto;
- se entro i suddetti termini il gestore non ha comunicato l'assunzione dell'incarico o non ha provveduto, ovvero non è possibile identificare il titolare o il gestore, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che provvede entro quarantotto ore dal ricevimento.

L'Istituto supporta le famiglie e i minori nella presentazione dell'istanza e conserva traccia dell'assistenza prestata.

4.4 Procedure operative e livelli di gestione

Le situazioni problematiche sono gestite da un team composto da: Dirigente Scolastico; Referente per il bullismo e il cyberbullismo; Animatore Digitale (PNSD); docenti referenti dell'educazione civica; psicologo o pedagogo ove disponibile.

La qualificazione del caso è **provvisoria** e viene aggiornata: "sospetto" non significa colpevolezza, "evidenza" non equivale a sentenza. Il Team evita confronti diretti tra vittima e presunto autore quando possano aumentare il rischio; la mediazione è valutata caso per caso e **non è automatica**.

Livello	Esempi	Azione
Preventivo	conflitto, uso improprio isolato, disagio non urgente	ascolto, intervento educativo, monitoraggio
Significativo	condotte reiterate, esclusione, molestie, diffusione lesiva	Team, famiglie ove appropriato, piano di tutela, possibile supporto specialistico
Urgente	minaccia, adescamento, immagini intime, autolesionismo, rischio attuale o possibile reato	protezione immediata, Dirigente, DPO se privacy, servizi/forze dell'ordine o autorità giudiziaria secondo competenza

La tabella dei livelli si coordina con la distinzione giuridica tra **sospetto** e **notizia di reato**:

CASO A — Sospetto (livello preventivo/significativo): il docente sospetta che tra gli studenti stia avvenendo qualcosa riconducibile a bullismo, cyberbullismo, sexting o adescamento online (indicatori indiretti, segnali di disagio, voci ricorrenti, cambiamenti di comportamento).

- Il docente compila la scheda di segnalazione (Allegato 1) in forma scritta, con dati e informazioni dettagliate e oggettive, e la trasmette al Referente e al Team Antibullismo;
- il Team valuta la segnalazione e allerta il Dirigente Scolastico;
- si avvia un'osservazione strutturata del gruppo classe, la valutazione pedagogica del caso e l'eventuale attivazione di percorsi di prevenzione, mediazione e sostegno, con coinvolgimento delle famiglie ove appropriato;
- si valuta se ricorrano gli estremi per l'invio della relazione agli organi giudiziari competenti;
- si dà conto dell'esito nella reportistica riservata.

CASO B — Evidenza / notizia di reato (livello urgente): il docente ha evidenza di una condotta conclamata riconducibile a bullismo, cyberbullismo, sexting o adescamento online (fatti circostanziati, testimonianze dirette, materiale digitale visionato), ovvero emergono elementi di possibile reato o grave pregiudizio.

- Il docente compila la scheda di segnalazione (Allegato 1) e la trasmette senza ritardo al Referente e al Dirigente Scolastico;
- il Dirigente Scolastico, salvo che il fatto costituisca reato, applica le procedure delle linee di orientamento: informa tempestivamente i genitori dei minori coinvolti, promuove iniziative educative e, nei casi più gravi o reiterati, riferisce alle autorità competenti per l'eventuale attivazione delle misure rieducative (art. 5 L. 71/2017; art. 2 L. 70/2024);
- se la condotta integra una fattispecie di reato perseguibile d'ufficio, si procede alla denuncia all'autorità giudiziaria competente (Procura ordinaria o minorile, Polizia Postale), senza svolgere indagini autonome e conservando le prove digitali;
- il Team convoca separatamente le famiglie dei minori coinvolti (vittime, autori, testimoni), garantendo l'ascolto protetto e la presa in carico educativa;

- ove ne ricorrano i presupposti e fino a quando non sia proposta querela o presentata denuncia, la famiglia del minore autore può essere informata della possibilità della procedura di ammonimento (art. 7 L. 71/2017);
- si redige il verbale di presa in carico (Allegato 2) e si programma il monitoraggio individuale.

Evidenze digitali: non cancellare, modificare o inoltrare chat, immagini o video; conservare l'originale soltanto nei limiti necessari, annotando fonte, data e modalità di acquisizione. Il personale non risponde al presunto adescatore, non crea copie diffuse e non effettua indagini tecniche. Nei casi di materiale sessualmente esplicito riguardante minori, non scaricare né redistribuire il contenuto e attivare immediatamente il Dirigente e le autorità competenti.

4.5 Strumenti di segnalazione

Sono disponibili: e-mail istituzionale dedicata [indirizzo da inserire]; segnalazione scritta al Dirigente o al Referente; box riservato; sportello di ascolto, se attivo; colloquio con docente di fiducia; canali nazionali di supporto indicati sul sito dell'Istituto (Helpline 19696, chat di Telefono Azzurro, 114 Emergenza infanzia, STOP-IT, Polizia Postale). I canali devono essere effettivamente attivati prima della pubblicazione del documento.

Chi riceve una segnalazione ascolta senza colpevolizzare, raccoglie solo le informazioni necessarie, registra data e fonte, informa tempestivamente il Dirigente e tutela la persona esposta al rischio. **Non promette anonimato assoluto quando la legge impone comunicazioni a soggetti competenti, ma garantisce la massima riservatezza compatibile con la tutela.**

Capitolo 5 — Monitoraggio e valutazione dell'ePolicy

L'ePolicy è un documento dinamico, soggetto a revisione periodica e miglioramento continuo.

Strumenti di rilevazione e indicatori: l'Istituto predispone questionari e checklist annuali rivolti a studenti, famiglie e personale per rilevare la percezione della sicurezza digitale e del clima scolastico, la frequenza e tipologia delle segnalazioni, la conoscenza degli strumenti di ascolto e la partecipazione alle attività formative.

Frequenza e responsabilità: la verifica è affidata al Team Antibullismo e per l'Emergenza, in collaborazione con il Referente d'Istituto e l'Animatore Digitale, e al tavolo permanente di monitoraggio (art. 4, comma 2-bis, L. 71/2017). Il Team redige una relazione almeno annuale con dati aggregati su attività formative, accesso ai canali, tempi medi di presa in carico, tipologie di rischio e azioni preventive: non sono riportati nomi, classi o dettagli che consentano l'identificazione dei minori. L'analisi dei dati avviene con cadenza semestrale e confluisce in una relazione finale presentata al Collegio dei Docenti e al Consiglio d'Istituto.

Revisione e aggiornamento: il documento è aggiornato con cadenza almeno annuale, o tempestivamente in caso di novità normative o di contesto, previa consultazione degli organi collegiali. Per ogni caso in carico sono previsti, ove appropriato, un controllo a 15 giorni e uno a 30-60 giorni, senza trasformare il monitoraggio in sorveglianza permanente.

Capitolo 6 — Responsabilità civile dell'Istituto e gestione del rischio

La prevenzione documentata non è solo un obiettivo educativo, ma uno strumento di gestione del rischio giuridico. I precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi nel tempo in cui sono sotto la loro vigilanza, e si liberano dalla responsabilità **soltanto se provano di non aver potuto impedire il fatto** (art. 2048, comma 2, c.c.).

Appendice — Glossario dei rischi online

- Bullismo: aggressione o molestia reiterate, anche in forma non telematica, idonee a provocare ansia, timore, isolamento o emarginazione (art. 1, comma 1-bis, L. 71/2017).
- Cyberbullismo: pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione o trattamento illecito di dati personali in danno di minorenni, realizzati per via telematica (art. 1, comma 2, L. 71/2017).

- Adescamento online (grooming): avvicinamento manipolatorio di un minore da parte di un adulto in rete, finalizzato alla commissione di reati sessuali.
- Sexting: invio o condivisione di immagini o video a contenuto sessualmente esplicito; la diffusione non consensuale può integrare il reato di cui all'art. 612-ter c.p.
- Flaming: invio di messaggi violenti e volgari.
- Denigrazione: diffusione di informazioni lesive della reputazione.
- Impersonation (furto d'identità): utilizzo dell'identità altrui per creare profili falsi o pubblicare contenuti.
- Outing: diffusione non autorizzata di informazioni intime o riservate.
- Esclusione: estromissione intenzionale da gruppi o attività online.
- Hate speech: discorsi d'odio fondati su razza, etnia, religione, genere, orientamento sessuale o disabilità.
- Datafication: riduzione di aspetti della vita a dati trattati algoritmicamente.
- Profilazione: costruzione di profili degli utenti sulla base dei dati raccolti.
- Netiquette: insieme delle regole per una comunicazione online rispettosa e corretta.
- Phishing: tentativo di ottenere dati personali o credenziali tramite messaggi ingannevoli.
- Malware: software dannoso (virus, spyware, ransomware) volto a compromettere dispositivi o dati.
- Identità digitale: insieme delle informazioni e delle tracce che rappresentano una persona negli ambienti digitali.

CODICE INTERNO PER LA PREVENZIONE E IL CONTRASTO DEI FENOMENI DI BULLISMO/CYBERBULLISMO

1. Riferimenti normativi e funzione

Il presente codice interno è adottato in conformità alle Linee di orientamento ministeriali e in attuazione dell'art. 4, comma 2-bis, L. 71/2017, ai sensi del quale ogni istituto scolastico, nell'ambito della propria autonomia, adotta un codice interno per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo e istituisce un tavolo permanente di monitoraggio.

Il codice opera in coordinamento con: la L. 71/2017 come modificata dalla L. 70/2024 (art. 1 L. 70/2024); l'art. 5 L. 71/2017 (ruolo del dirigente scolastico e integrazione del regolamento e del Patto di corresponsabilità); il Regolamento d'Istituto, il Regolamento di disciplina e il Patto educativo di corresponsabilità; la presente ePolicy, di cui costituisce parte integrante. In caso di contrasto, prevalgono la legge e i regolamenti vigenti.

2. Definizioni

Ai fini del presente codice:

- per bullismo si intendono "l'aggressione o la molestia reiterate, da parte di una singola persona o di un gruppo di persone, in danno di un minore o di un gruppo di minori, idonee a provocare sentimenti di ansia, di timore, di isolamento o di emarginazione, attraverso atti o comportamenti vessatori, pressioni o violenze fisiche o psicologiche, istigazione al suicidio o all'autolesionismo, minacce o ricatti, furti o danneggiamenti, offese o derisioni" (art. 1, comma 1-bis, L. 71/2017);

- per cyberbullismo 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 online aventi ad oggetto anche uno o più componenti della famiglia del minore, il cui scopo intenzionale e predominante sia isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso o la loro messa in ridicolo (art. 1, comma 2, L. 71/2017).

3. Ambito di applicazione e destinatari

Il codice si applica alle attività scolastiche in presenza e a distanza, alle reti e piattaforme dell'Istituto, ai dispositivi personali utilizzati per finalità didattiche e alle attività esterne organizzate o autorizzate dalla scuola. Si rivolge a studentesse e studenti, personale docente e ATA, famiglie, collaboratori ed esperti esterni, enti e associazioni che operano con l'Istituto.

4. Principi generali

- Interesse superiore del minore: ogni intervento privilegia la protezione e il benessere del minore, in linea con l'art. 3 della Convenzione ONU sui diritti del fanciullo, ratificata con L. 176/1991 (Cass. civ., Sez. I, n. 23669/2023).
- Finalità educativa e riparativa: gli interventi privilegiano azioni formative ed educative, anche con percorsi di mediazione scolastica e attività riparatorie, fermi restando gli obblighi di legge.
- Proporzionalità e gradualità: le sanzioni disciplinari sono commisurate alla gravità degli atti compiuti e graduate, nel rispetto del Regolamento di disciplina.
- Riservatezza: i dati e le segnalazioni sono trattati secondo il criterio di stretta necessità, nel rispetto del GDPR e del D.Lgs. 196/2003; non è promesso anonimato assoluto quando la legge impone comunicazioni a soggetti competenti.
- Non colpevolezza presunta: "sospetto" non significa colpevolezza e "evidenza" non equivale a sentenza; la qualificazione dei casi è provvisoria e aggiornabile.
- Divieto di indagini autonome: il personale non svolge attività investigativa, non interroga informalmente i minori in modo suggestivo, non contatta il presunto autore online e non inoltra materiale illecito.

5. Condotte richieste

Gli studenti sono tenuti a: rispettare persone, dati, dispositivi e regole di rete; utilizzare le tecnologie per finalità didattiche e in modo rispettoso; proteggere le proprie credenziali; segnalare in forma riservata eventuali situazioni di rischio proprie o di compagni; partecipare alle attività di prevenzione e di peer education.

Il personale è tenuto a: osservare e prevenire le condotte a rischio; segnalare tempestivamente al Dirigente e al Referente; seguire le procedure dell'ePolicy; partecipare alla formazione.

Le famiglie collaborano con la scuola, partecipano ai momenti formativi e segnalano le criticità, senza sostituirsi ai soggetti istituzionali.

6. Condotte vietate

Sono vietati, in forma telematica e non, tra l'altro: aggressioni e molestie reiterate; vessazioni, pressioni e violenze fisiche o psicologiche; minacce, ricatti, offese e derisioni; istigazione al suicidio o all'autolesionismo; furto d'identità e creazione di profili falsi; diffusione non consensuale di immagini, audio, video o dati personali; diffusione di contenuti discriminatori o di incitamento all'odio; consultazione o diffusione di materiale illecito; danneggiamento di dispositivi o alterazione

delle configurazioni di rete. La violazione comporta l'applicazione delle sanzioni previste dal Regolamento di disciplina, commisurate alla gravità, ferme le conseguenze civili e penali.

7. Sistema di prevenzione

Il Liceo attua: il curriculum di educazione civica digitale (L. 92/2019; DigComp 2.2); le attività del Safer Internet Day, della Giornata del rispetto (20 gennaio, art. 4 L. 70/2024) e della Giornata nazionale contro il bullismo e il cyberbullismo (7 febbraio); il kit didattico di Generazioni Connesse; i percorsi di peer education sotto supervisione adulta; la formazione di docenti, studenti e famiglie; lo Sportello di ascolto e il raccordo con il servizio di sostegno psicologico eventualmente attivato dalla Regione ai sensi dell'art. 4-bis L. 71/2017.

8. Procedura di segnalazione

Per la segnalazione e la gestione dei casi si applicano integralmente le procedure del Capitolo 4 dell'ePolicy (casi di sospetto e di evidenza, livelli di gestione, obblighi di denuncia, procedura di oscuramento ex art. 2 L. 71/2017, misure rieducative ex art. 25 R.D.L. 1404/1934 come riformato dall'art. 2 L. 70/2024, ammonimento ex art. 7 L. 71/2017).

9. Misure educative e sanzioni

Le sanzioni disciplinari sono applicate secondo il Regolamento di disciplina, con contestazione, valutazione individuale, proporzionalità, possibilità di difesa e competenza dell'organo previsto. Le misure educative e riparative (percorsi di mediazione, attività di utilità sociale, laboratori) possono affiancare o precedere le sanzioni. Nei casi più gravi o reiterati, il Dirigente riferisce alle autorità competenti anche per l'eventuale attivazione delle misure rieducative di cui all'art. 25 R.D.L. 1404/1934, come riformato (art. 2 L. 70/2024).

10. Tavolo permanente di monitoraggio

Il tavolo permanente di monitoraggio, istituito ai sensi dell'art. 4, comma 2-bis, L. 71/2017, è composto da rappresentanti degli studenti, degli insegnanti, delle famiglie ed esperti di settore (psicologo o pedagogista ove disponibile, referenti degli enti locali e delle associazioni territoriali). Il tavolo: monitora le segnalazioni e i relativi esiti; verifica l'efficacia delle azioni di prevenzione; propone aggiornamenti del presente codice e dell'ePolicy; promuove la cultura del rispetto e della non violenza. Si riunisce almeno due volte l'anno e redige una sintesi delle attività per il Collegio dei Docenti e il Consiglio d'Istituto.

11. Approvazione e revisione

Il codice è esaminato dagli organi collegiali competenti, coordinato con il Regolamento d'Istituto e il Patto educativo di corresponsabilità, e sottoposto al DPO per le parti relative alla protezione dei dati personali. La versione pubblicata riporta data, numero di versione, delibera di adozione, allegati vigenti e data prevista per il riesame. Il codice è riesaminato almeno annualmente, e comunque in caso di novità normative o di contesto.