



ISTITUTO COMPRENSIVO STATALE - N. 9-FORLI'
Prot. 0007485 del 27/06/2025
I (Uscita)



Istituto Comprensivo N. 9
“BEATRICE PORTINARI”

Via Lughese, 113 - San Martino Villafranca – 47122 FORLÌ (FC) Tel. 0543/36221
C.F.:92089450404 - Cod. Mecc. FOIC820007 - CODICE UNIVOCO: UF8I7H
e-mail: foic820007@istruzione.it pec: foic820007@pec.istruzione.it

Documento di ePolicy

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

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

Capitolo 2 - Sensibilizzazione e prevenzione

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

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

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

Capitolo 4 - Segnalazione e gestione dei casi

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

1.1 Scopo dell'ePolicy

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

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

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

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

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

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

Un ePolicy per l'IC9

Nel nostro Istituto il documento di ePolicy ha lo scopo di promuovere le competenze digitali ed un uso delle tecnologie digitali positivo, critico e consapevole, sia da parte degli studenti che delle studentesse che da parte dell'intera comunità educante.

Inoltre attraverso il documento E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet. L'E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

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

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

Affinché l'ePolicy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

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

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

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

promuovere la cultura della sicurezza online e garantirla a tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento, le indicazioni del MIM, delle sue agenzie e attraverso il documento di ePolicy; promuovere la cultura della sicurezza online – anche attraverso il documento di ePolicy - integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;

ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, i suoi strumenti ed ambienti e deve garantire alla popolazione scolastica la sicurezza di navigazione tramite internet utilizzando adeguati sistemi informatici e filtri;

ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segua le pratiche migliori possibili nella gestione dei dati stessi;

deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;

ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;

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

deve essere a conoscenza ed attuare le procedure necessarie in caso di grave incidente di sicurezza online.

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

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

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

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

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

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

Il Team ha il compito di:

coadiuvare il Dirigente scolastico, coordinatore del Team, nella definizione degli interventi di prevenzione del bullismo (per questa funzione partecipano anche il presidente del Consiglio d'Istituto e i Rappresentanti degli studenti).

Intervenire (come gruppo ristretto, composto da Dirigente e referente o referenti per il bullismo e il cyberbullismo, psicologo o pedagogo, se presente) nelle situazioni acute di bullismo.

Promuovere la redazione e l'applicazione della ePolicy e monitorare le segnalazioni.

I/LE DOCENTI

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

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

RESPONSABILE DELLA PROTEZIONE DEI DATI

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

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

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

GLI STUDENTI E LE STUDENTESSE

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

I rappresentanti degli/delle studenti sono informati del documento di ePolicy e invitati a costruire i piani di azione, a partire

Documento di ePolicy - IC N. 9 - FORLÌ - 19/06/2025 - 15:25 Pagina: 5/32
dal secondo anno della secondaria di II grado,

I GENITORI/ADULTI DI RIFERIMENTO

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

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

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

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

a. Informativa per i docenti interni che organizzano corsi o attività all'interno del nostro Istituto

Attenzione e Vigilanza

Nel caso di sospetti comportamenti scorretti da parte degli studenti è fondamentale che il docente intervenga tempestivamente segnalando il sospetto in modo dettagliato in forma scritta al referente per il cyberbullismo o al team di docenti specializzati.

Questo team, una volta raccolta appunto tale segnalazione, la discute e la condivide con il dirigente scolastico. Insieme si valuta attentamente il caso e si decide eventualmente se è necessario coinvolgere organi spettro giudiziari o di pianificare azioni di sensibilizzazione mirate.

b. Informativa per i soggetti esterni eroganti corsi o attività all'interno dell'Istituto

Ascolto e Attenzione

Tutte le persone della nostra comunità scolastica che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal

principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa. Sono vietati i comportamenti irrispettosi, offensivi o lesivi

Documento di ePolicy - IC N. 9 - FORLI' - 19/06/2025 - 15:25 Pagina: 6/32

della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

c. Informativa per gli STUDENTI che hanno accesso alle tecnologie informatiche della scuola e alla piattaforma.

Responsabilità e sanzioni

Con riferimento al capitolo 3.2 , art9 del Regolamento Gsuite di questo documento, in merito ai comportamenti corretti in rete, nello specifico con l'utilizzo dell'account con dominio scolastico si riporta quanto segue:

"Art. 9

(Infrazioni e sanzioni)

a. In caso di violazione delle norme stabilite nel presente Regolamento, l'Istituto, nella persona del suo rappresentante legale, il Dirigente Scolastico, e/o dell'Amministratore potrà sospendere

l'account dell'utente o revocarlo definitivamente senza alcun preavviso e senza alcun addebito a

suo carico e fatta salva ogni altra azione di rivalsa nei confronti dei responsabili delle violazioni. b.

Qualsiasi violazione del presente regolamento, di quelli di istituto nonché della legislazione

vigente, connessa all'uso dell'account sarà sanzionata nelle modalità stabilite dai regolamenti

dell'istituto.

c. L'Istituto si riserva la facoltà di segnalare alle autorità competenti - per gli opportuni accertamenti ed

i provvedimenti del caso - le eventuali violazioni alle condizioni di utilizzo indicate nel presente

Regolamento, oltre che alle leggi ed ai regolamenti vigenti."

Nello specifico in merito ai documenti sanzionatori:

Il regolamento di Istituto prevede sanzioni disciplinari riguardo ai seguenti comportamenti ritenuti di particolare gravità:

Utilizzo del cellulare negli ambienti scolastici

Violazione della privacy con mezzi audio-visivi

Atti di bullismo e tutti gli atti di violenza fisica, verbale e morale

Comportamenti che configurano ipotesi di reato

Inoltre in riferimento alla circolare dell'Istituto con prot 0002652 del 13/03/2025

Si ricorda che la **circolare del Ministero dell'Istruzione e del Merito N. 5274 dell'11 luglio 2024** " Disposizioni in merito

all'uso degli smartphone e del registro elettronico nel primo ciclo di istruzione - A.S. 2024 -2025", dispone il divieto di utilizzo in classe del telefono smartphone, anche a fini educativi e didattici, per gli alunni dalla scuola d'infanzia fino alla secondaria di primo grado, salvo i casi in cui lo stesso sia previsto dal Piano educativo individualizzato o dal Piano didattico personalizzato, come supporto rispettivamente agli alunni con disabilità o con disturbi specifici di apprendimento ovvero per

Documento di ePolicy - IC N. 9 - FORLI' - 19/06/2025 - 15:25 Pagina: 7/32
documentate e oggettive condizioni personali.

1.3 Integrazione ePolicy nei documenti scolastici

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

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

Il Regolamento dell'Istituto scolastico, che rappresenta il principale punto di riferimento normativo, dovrà essere aggiornato in modo tale da dare contezza dell'adozione dell'ePolicy, e richiamare le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione in ambiente scolastico.

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

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

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

Il documento di ePolicy del nostro Istituto viene integrato al PTOF e linkato al patto di corresponsabilità.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curricolo sulle competenze digitali per la comunità educante (il DigComp2.2);
2. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle

Documento di ePolicy - IC N. 9 - FORLI' - 19/06/2025 - 15:25 Pagina: 8/32
tecnologie digitali con relative informative;

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

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

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

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

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

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

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

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

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

Il documento di ePolicy del nostro Istituto viene approvato in Collegio Docenti e in Consiglio di Istituto, pubblicato sul sito della scuola nella sezione dedicata al PTOF e nella sezione dedicata al Cyberbullismo al fine di una comunicazione e condivisione trasparente con l'intera comunità educante.

1.5 - I Piani di Azione dell'ePolicy

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

Documento di ePolicy - IC N. 9 - FORLÌ - 19/06/2025 - 15:25 Pagina: 9/32

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

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

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

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

MODULO II

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

MODULO III

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

MODULO IV

- Definizione, a partire da quanto definito nell'ePolicy, delle procedure di segnalazione anche con linguaggio child/youth

friendly perché possano essere accessibili a studenti e studentesse;
Realizzare una reportistica delle segnalazioni ricevute e dei relativi esiti.

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

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

Documento di ePolicy - IC N. 9 - FORLI' - 19/06/2025 - 15:25 Pagina: 10/32
MODULO II

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

Realizzare una formazione rivolta agli studenti e alle studentesse attraverso il percorso previsto sulla piattaforma di Generazioni Connesse;

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

Nello specifico per l'Istituto Comprensivo 9 Beatrice portinari

1° ANNO DI ATTIVITA' CON L'EPOLICY a.s. 2025/2026

MODULO I

Presentazione dell'ePolicy ai docenti durante il collegio docenti conclusivo dell'a.s.2024/25;

Realizzare un evento di diffusione dell'ePolicy in occasione degli Open Day;

Diffondere l'ePolicy negli ambienti scolastici, a studenti e studentesse, docenti e famiglie attraverso il link al patto di corresponsabilità;

MODULO II

Effettuare una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale;

Effettuare una rilevazione di interessi, bisogni e comportamenti delle famiglie sull'uso positivo del digitale;

Avviare l'introduzione del kit didattico come metodo e risorsa di lavoro in alcune classi pilota;

MODULO III

Integrare l'ePolicy (norme, regolamenti e procedure) nei documenti dell'Istituto;

Aggiornare i regolamenti d'Istituto e creare il curriculum digitale

Documento di ePolicy - IC N. 9 - FORLÌ - 19/06/2025 - 15:25 Pagina: 11/32

2° ANNO DI ATTIVITA' CON L'EPOLICY 2026/27

MODULO I

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

MODULO II

L'Istituto utilizza il kit didattico come pratica metodologica e risorse a disposizione dei docenti attraverso il sito di Generazioni Connesse;

Effettuare una rilevazione di interessi, bisogni, comportamenti, abitudini di studenti e studentesse sui temi dell'educazione civica digitale;

Realizzare una formazione rivolta alle famiglie.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

[Kit Didattico](#)

Area formazione (per docenti, famiglie, studenti/sse con ePolicy)

Canale [Youtube](#) (webinar, video-stimolo, serie per target differenti)

Canale [TikTok](#)

Canale [Instagram](#)

Canale [Facebook](#)

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

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

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

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

Pertanto l'Istituto riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (ad es. con l'aiuto dell'animatore digitale), dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online) sulle TIC e si impegna a organizzare ogni anno momenti di formazione sui metodi e sugli strumenti della didattica digitale.

2.2 - Il Curricolo Digitale

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

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

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

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

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

Documento di ePolicy - IC N. 9 - FORLÌ - 19/06/2025 - 15:25 Pagina: 13/32

CURRICULO SCUOLA PRIMARIA E SECONDARIA DI PRIMO GRADO con riferimento alle Indicazioni Nazionali 2012

COMPETENZA DIGITALE

COMPETENZA DIGITALE

DISCIPLINA DI RIFERIMENTO: tutte

DISCIPLINE CONCORRENTI: tutte

La competenza digitale è ritenuta dall'Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d'oggi. L'approccio per discipline scelto dalle Indicazioni non consente di declinarla con le stesse modalità con cui si possono declinare le competenze chiave nelle quali trovano riferimento le discipline formalizzate. Si ritrovano abilità e conoscenze che fanno capo alla competenza digitale in tutte le discipline e tutte concorrono a costruirla. Competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnanti sono coinvolti nella sua costruzione.

SEZIONE A: Traguardi formativi				
COMPETENZA CHIAVE EUROPEA:	COMPETENZA DIGITALE			
Fonti di legittimazione:	Raccomandazione del Parlamento Europeo e del Consiglio 18.12.2006 Indicazioni Nazionali per il Curriculum 2012			
	FINE CLASSE TERZA SCUOLA PRIMARIA		FINE SCUOLA PRIMARIA	
COMPETENZE SPECIFICHE		CONOSCENZE	ABILITÀ	CONOSCENZE

Documento di ePolicy - IC N. 9 - FORLÌ - 19/06/2025 - 15:25 Pagina: 14/32

Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio. Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate.	Utilizzare nelle funzioni principali televisore, video, telefono e telefonino Spiegare le funzioni principali e il funzionamento elementare degli apparecchi per la comunicazione e l'informazione. Utilizzare il PC, con la supervisione dell'insegnante, per scrivere compilare tabelle. Utilizzare alcune funzioni principali, come creare un file, caricare immagini, salvare il file. Individuare alcuni rischi fisici nell'uso di apparecchiature elettriche ed elettroniche e ipotizzare soluzioni preventive. Individuare alcuni rischi nell'utilizzo della rete Internet e ipotizzare alcune semplici soluzioni preventive.	I principali strumenti per l'informazione e la comunicazione: televisore, lettore video e CD/DVD, apparecchi telefonici fissi e mobili, PC Funzioni principali degli apparecchi per la comunicazione e l'informazione Funzionamento elementare dei principali apparecchi elettrici ed elettronici Rischi nell'utilizzo di apparecchi elettrici ed elettronici Rischi nell'utilizzo della rete con PC e telefonini	Utilizzare consapevolmente le più comuni tecnologie, conoscendone i principi di base soprattutto in riferimento agli impianti domestici. Utilizzare semplici materiali digitali per l'apprendimento. Utilizzare il PC, alcune periferiche e programmi applicativi. Avviare alla conoscenza della Rete per scopi di informazione, comunicazione, ricerca e svago. Individuare rischi fisici nell'utilizzo delle apparecchiature elettriche ed elettroniche e i possibili comportamenti preventivi. Individuare i rischi nell'utilizzo della rete Internet e alcuni comportamenti preventivi e correttivi.	Semplici applicazioni tecnologiche quotidiane e relative modalità di funzionamento I principali dispositivi informatici di input e output I principali software applicativi utili per lo studio, con particolare riferimento alla videoscrittura, alle presentazioni e ai giochi didattici Semplici procedure di utilizzo di Internet per ottenere dati, fare ricerche, comunicare Rischi fisici nell'utilizzo di apparecchi elettrici ed elettronici Rischi nell'utilizzo della rete con PC e telefonini
--	---	--	---	--

SEZIONE A: Traguardi formativi		
COMPETENZA CHIAVE EUROPEA:	COMPETENZA DIGITALE	
Fonti di legittimazione:	Raccomandazione del Parlamento Europeo e del Consiglio 18.12.2006 Indicazioni Nazionali per il Curricolo 2012	
	FINE SCUOLA SECONDARIA DI PRIMO GRADO	
COMPETENZE SPECIFICHE	ABILITÀ	CONOSCENZE

Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio. Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate.	Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti in diverse situazioni. Conoscere gli elementi basilari che compongono un computer e le relazioni essenziali fra di essi. Collegare le modalità di funzionamento dei dispositivi elettronici con le conoscenze scientifiche e tecniche acquisite. Utilizzare materiali digitali per l'apprendimento. Utilizzare il PC, periferiche e programmi applicativi Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago. Riconoscere potenzialità e rischi connessi all'uso delle tecnologie più comuni, anche informatiche.	Le applicazioni tecnologiche quotidiane e le relative modalità di funzionamento I dispositivi informatici di input e output Il sistema operativo e i più comuni software applicativi, con particolare riferimento all'office automation e ai prodotti multimediali anche Open source Procedure per la produzione di testi, ipertesti, presentazioni e utilizzo dei fogli di calcolo Procedure di utilizzo di reti informatiche per ottenere dati, fare ricerche, comunicare Caratteristiche e potenzialità tecnologiche degli strumenti d'uso più comuni Procedure di utilizzo sicuro e legale di reti informatiche per ottenere dati e comunicare (motori di ricerca, sistemi di comunicazione mobile, email, chat, social network, protezione degli account, download, diritto d'autore, ecc.) Fonti di pericolo e procedure di sicurezza
--	--	--

3

SEZIONE B: Livelli di padronanza				
COMPETENZA CHIAVE EUROPEA:	COMPETENZA DIGITALE			
LIVELLI DI PADRONANZA				
1	2	3	4	5

Sottoladiretta supervisione dell'insegnante identifica, denomina e conosce le funzioni fondamentali di base dello strumento; con la supervisione dell'insegnante, utilizza i principali componenti, in particolare la tastiera. Comprende e produce semplici frasi associandole ad immagini date.	Sottoladiretta supervisione dell'insegnante e con sue istruzioni, scrive un semplice testo al computer e lo salva. Comprende semplici testi inviati da altri via mail; con l'aiuto dell'insegnante, trasmette semplici messaggi di posta elettronica. Utilizza la rete solo con la diretta supervisione dell'adulto per cercare informazioni.	Scrivo, revisiono e archivio in modo autonomo testi scritti con il calcolatore. Costruisce tabelle di dati con la supervisione dell'insegnante; utilizza fogli elettronici per semplici elaborazioni di dati e calcoli, con istruzioni. Confeziona e invia autonomamente messaggi di posta elettronica rispettando le principali regole della netiquette. Accede alla rete con la supervisione dell'insegnante per ricavare informazioni. Conosce e descrive alcuni rischi della navigazione in rete e dell'uso del telefonino e adotta i comportamenti preventivi.	Scrivo, revisiono e archivio in modo autonomo testi scritti con il calcolatore; è in grado di manipolarli, inserendo immagini, disegni, anche acquisiti con lo scanner, tabelle. Costruisce tabelle di dati; utilizza fogli elettronici per semplici elaborazioni di dati e calcoli. Utilizzo la posta elettronica e accedo alla rete con la supervisione dell'insegnante per ricavare informazioni e per collocarle di proprie. Conosco e descrivo i rischi della navigazione in rete e dell'uso del telefonino e adotto i comportamenti preventivi.	Utilizzo in autonomia programmi di videoscrittura, fogli di calcolo, presentazioni per elaborare testi, comunicare, eseguire compiti e risolvere problemi. So utilizzare la rete per reperire informazioni, con la supervisione dell'insegnante; organizzo le informazioni in file, schemi, tabelle, grafici; collego file differenti. Confronto le informazioni reperite in rete anche con altre fonti documentali, testimoniali, bibliografiche. Comunico autonomamente attraverso la posta elettronica. Rispetto le regole della netiquette nella navigazione in rete e so riconoscere i principali pericoli della rete (spam, falsi messaggi di posta, richieste di dati personali, ecc.), contenuti pericolosi o fraudolenti, evitandoli.
--	--	--	--	---

Livello 3: atteso a partire dalla fine della scuola primaria Livello 4: atteso nella scuola secondaria di primo grado
Livello 5: atteso alla fine della scuola secondaria di primo grado 4

2.3 - Il Kit Didattico

L'e-Policy prevede, a livello macro, un lavoro di lettura e d'intenti condivisi dall'intera comunità scolastica, a livello micro, invece, immagina che la singola classe lavori anche su tematiche direttamente collegate alla sicurezza in rete, ma complesse e di non

immediata ricaduta nelle programmazioni scolastiche (etica e digitale, algoritmi, datafication). A tal fine si è progettato e predisposto del materiale che possa funzionare sia da attivatore, sia d'accompagnamento ai docenti e agli studenti nella fase più delicata ed incisiva del processo di prevenzione: la lezione in classe.

Pertanto, il progetto Generazioni Connesse, a supporto del lavoro dell'e-Policy ha previsto per i docenti e studenti di ogni

Documento di ePolicy - IC N. 9 - FORLI' - 19/06/2025 - 15:25 Pagina: 17/32

segmento scolare un nuovo [Kit Didattico](#) che contiene materiali per le lezioni e per il proprio aggiornamento, a partire dalla scuola d'infanzia fino alla secondaria di secondo grado. Il Kit può essere usato nella sua interezza oppure può essere oggetto di selezione e scelta, sulla base di quanto fatto dal docente.

L'Istituto si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti. La scuola invita tutti i docenti a effettuare la formazione sul sito Generazioni Connesse.

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

3.1 - Protezione dei dati personali e GDPR

La protezione dei dati personali delle persone fisiche costituisce un diritto fondamentale. L'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE»)

stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Le principali normative di riferimento sono il Regolamento Generale sulla Protezione dei Dati 2016/679 noto anche come GDPR, e il Dlgs 196/2003 conosciuto come Codice Privacy.

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

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

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

Le istituzioni scolastiche pubbliche possono trattare soltanto i **dati personali necessari al perseguimento delle specifiche finalità istituzionali**, che sono comunque **finalità di rilevante interesse pubblico**, in ossequio ai principi di [finalità](#) e non eccedenza, oppure quelli espressamente previsti dalla normativa di settore. Non possono essere chiesti dati non rilevanti per la finalità istituzionali. Quindi, per tali trattamenti non occorre il [consenso](#) degli studenti, la [base giuridica del trattamento](#) è, infatti, data dall'**interesse pubblico**.

Occorre, ovviamente, particolare [cautela nel trattamento](#) dei dati, trattandosi di dati relativi a soggetti generalmente minorenni. In alcuni casi si tratta anche di [dati a trattamento speciale](#), cioè relativi alla salute o giudiziari. In questo caso le cautele devono essere massime e soprattutto occorre verificare se il trattamento di quei dati sia davvero necessario per il perseguimento delle finalità scolastiche.

Chi è il "Responsabile della Protezione dei Dati (RPD)"?

Qualità, caratteristiche e compiti del Responsabile della Protezione dei Dati sono previsti e disciplinati dagli articoli 37, 38 e 39 del Regolamento europeo n. 679/2016 e ben chiariti dalle Linee-guida sui responsabili della protezione dei dati adottate in data 13 dicembre 2016 dal Gruppo di lavoro Articolo 29 in materia di protezione dei dati personali oltreché da diverse recenti FAQ del Garante per la protezione dei dati personali.

Il Responsabile della Protezione dei Dati (RPD) ha una funzione generale di sorvegliare che l'Ente svolga la sua attività nel rispetto della normativa in materia di protezione dei dati personali.

In particolare, ha anche una funzione di punto di contatto-riferimento per i cittadini rispetto a problematiche e questioni relative al trattamento dei loro dati personali da parte dell'Ente e al rispetto dei loro diritti in materia.

Documento di ePolicy - IC N. 9 - FORLÌ - 19/06/2025 - 15:25 Pagina: 19/32

Dati del Responsabile della Protezione dei Dati: **Ing. Enrica Marsiglio** presso S&L srl, via Bovini n. 41 – 48123 Ravenna (RA)

Il Responsabile della Protezione dei Dati (RPD) è sempre raggiungibile all'indirizzo del titolare e all'email:
privacy@sicurezzaoggi.com, sicurezzaoggi2@pec.it

3.2 - Strumenti di comunicazione online (PUA)

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

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



REGOLAMENTO PER L'UTILIZZO PIATTAFORMA

“G SUITE FOR EDUCATION” per L'Istituto Comprensivo 9.

Documento di ePolicy - IC N. 9 - FORLÌ - 19/06/2025 - 15:25 Pagina: 20/32

Il presente regolamento disciplina l'uso del Servizio della piattaforma “Google Suite for Education”

attivata dall'Istituto Scolastico come supporto alla didattica ed alla comunicazione interna ed esterna. Il

regolamento si applica a tutti gli utenti titolari di un account (direzione, docenti, studenti, personale Ata).

Copia del regolamento è pubblicata sul sito web d'istituto: <https://www.ic9forli.edu.it/> **Art. 1**

(Definizioni)

Nel presente Regolamento, i termini qui sotto elencati hanno il seguente significato:

a. Istituto: Istituto Comprensivo n.9 “Beatrice Portinari” di Forlì;

b. Amministratore di dominio: l'incaricato dal Dirigente Scolastico per l'amministrazione del servizio.

c. Servizio: servizio "G Suite for Education" messo a disposizione dall'Istituto. d. Fornitore:

Google Inc., con sede 1600 Amphitheatre Parkway Mountain View, CA 94043 Stati Uniti.

e. Utente: colui che utilizza un account del cui uso è pienamente responsabile. f. Account: insieme di funzionalità, applicativi, strumenti e contenuti attribuiti ad un nome utente con le credenziali di accesso.

Art. 2

(Natura e finalità del servizio)

Il servizio consiste nell'accesso agli applicativi di "G Suite for Education" del fornitore. L'istituto utilizza server Google per l'erogazione del servizio oggetto del presente Regolamento, su tali server ogni utente avrà a disposizione una casella di posta elettronica, oltre alla possibilità di utilizzare tutti i servizi di G Suite for Education (Google Drive, Documenti Google, Moduli, Google Classroom, ecc.) senza la necessità di procedere ad alcuna installazione per la loro funzionalità (cloud). Il servizio è inteso come supporto alla didattica e ai servizi correlati con le attività scolastiche in generale. Pertanto, gli account creati devono essere usati esclusivamente per tali fini.

La casella è strettamente personale e non è ammesso l'utilizzo da parte di persone diverse dall'assegnatario, né questi può cederla a terzi. L'utente, pertanto, accetta di essere riconosciuto quale autore dei messaggi inviati dal suo account e di essere il ricevente dei messaggi spediti al suo account.

Documento di ePolicy - IC N. 9 - FORLÌ - 19/06/2025 - 15:25 Pagina: 21/32

Le credenziali di accesso per gli studenti al servizio saranno:

USER: nomecognome@ic9forli.edu.it

* tutto minuscolo

* apostrofi e spazi per nomi o cognomi composto vanno omessi

PASSWORD: PROVVISORIA

* con obbligo di modifica al primo accesso

Il servizio mette a disposizione dell'utente una serie di applicazioni dette APP (attivabili o meno a discrezione dall'Istituto) utilizzabili via internet per le esigenze legate all'attività svolta, secondo regole e

limiti definite di volta in volta dall'Istituto, indipendentemente dalle possibilità tecniche offerte dalla piattaforma di Google. Il servizio è fornito gratuitamente ed è fruibile fino al termine del percorso di studio degli studenti o al termine dell'attività lavorativa presso l'Istituto del personale. **Art. 3**

(Soggetti che possono accedere al servizio in qualità di utenti)

A tutto il personale in servizio e agli studenti regolarmente iscritti verrà creato un account. Altre categorie di utenti possono richiedere la creazione di un account, sempre in relazione alle necessità didattiche e di comunicazione; in questo caso l'accoglimento della domanda indirizzata al Dirigente è a insindacabile giudizio del responsabile.

Art. 4

(Condizioni e norme di utilizzo)

Per tutti gli utenti l'attivazione del servizio è subordinata all'accettazione esplicita del presente Regolamento.

a. L'utente può accedere direttamente al suo account istituzionale collegandosi a Google.it, inserendo le credenziali utente fornita inizialmente dall'Amministratore che sarà necessario modificare al primo accesso.

b. Gli account fanno parte del dominio @ic9forli.edu.it di cui l'Istituto è proprietario. c.

L'utente potrà cambiare in ogni momento la password di accesso.

d. Nel caso di smarrimento della password, l'utente dovrà richiedere per iscritto il reset della password per il rilascio di una nuova password momentanea da cambiare al primo nuovo accesso.

Documento di ePolicy - IC N. 9 - FORLI' - 19/06/2025 - 15:25 Pagina: 22/32

e. L'utente s'impegna a non utilizzare il servizio per effettuare azioni e/o comunicazioni che arrechino danni o turbative alla rete o a terzi utenti o che violino le leggi ed i regolamenti d'Istituto vigenti.

f. Egli s'impegna anche a rispettare le regole che disciplinano il comportamento nel rapportarsi con altri utenti e a non ledere i diritti e la dignità delle persone.

g. Gli utenti si impegnano, altresì, al rispetto delle norme di buon utilizzo del servizio ed in particolare si impegnano a:

- non trasmettere, distribuire, condividere o mantenere qualsiasi tipo di materiale che violi qualsiasi legge o regolamento in vigore. Questo include, senza limitazioni, materiale protetto

da copyright, marchi registrati, segreti industriali o altre proprietà intellettuali, materiale pornografico, diffamatorio o che costituisce trattamento illecito di dati personali o viola le leggi sul controllo delle esportazioni;

- non procedere all'invio massivo di mail non richieste (spam). La spedizione di qualsiasi forma di spam attraverso il servizio di posta fornito è proibita. Gli account forniti non possono essere utilizzati per raccogliere risposte a messaggi spediti da altri Internet Service Provider, se questi messaggi violano il presente regolamento.

- non fare pubblicità a nessun tipo di prodotto o servizio; a non pubblicizzare, trasmettere o altrimenti rendere disponibile qualsiasi tipo di software, programma, prodotto o servizio che viola il presente regolamento o la legge vigente.

h. L'utente, inoltre, si impegna a non divulgare messaggi di natura ripetitiva ("catene di S. Antonio") anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus); a fronte di tale evenienza l'utente è tenuto a segnalarla al Dirigente scolastico e/o all'Amministratore.

i. Ogni singolo utente mallevera l'Istituto, sostanzialmente e processualmente, sollevandolo da ogni responsabilità, danno, arrecato a sé stesso o a terzi, costo o spesa, incluse le spese legali, derivanti da ogni violazione delle suddette norme.

j. Per nessun motivo, l'account e la mail ad esso associato possono essere utilizzati per acquisti e transazioni.

k. Per nessun motivo, l'account, la mail e i servizi ad esso associati possono essere utilizzati per

Documento di ePolicy - IC N. 9 - FORLÌ - 19/06/2025 - 15:25 Pagina: 23/32
motivi non strettamente collegati alle attività istituzionali che dipendono dal ruolo rivestito

all'interno dell'Istituto (docenti, personale A.T.A).

l. Accettando il presente Regolamento, l'utente accetta anche le norme sulla privacy di Google reperibili agli indirizzi <https://www.google.com/intl/it/policies/privacy/> e https://gsuite.google.com/terms/education_privacy.html

Articolo 5

(Credenziali di accesso)

Al primo accesso l'utente accede con la password: PROVVISORIA.

Tale password andrà obbligatoriamente cambiata al primo accesso e gelosamente custodita. Se l'utente perde ripetutamente la password verrà sanzionato.

Articolo 6

(Attivazione account studenti)

A settembre, a tutti agli studenti regolarmente iscritti al primo anno o trasferiti da altra scuola verrà creato un account con dominio @ic9forli.edu.it.

Gli studenti potranno utilizzare i Servizi principali di G-Suite

(https://gsuite.google.com/intl/it/terms/user_features.html).

Lo spazio virtuale offerto agli studenti può essere utilizzato esclusivamente per ospitare materiale didattico in accordo con quanto stabilito dagli insegnanti. Non è consentito utilizzare l'account per gestire ed archiviare immagini, file o documenti personali. Ogni comportamento scorretto ed ogni violazione saranno sanzionati.

Art. 7

(Cessazione del servizio Google Suite)

a. Per gli studenti - Il servizio viene reso disponibile agli studenti per tutto il periodo di iscrizione presso l'Istituto e cesserà al termine del l'ultimo anno, oppure qualora lo studente cambiasse scuola. Sarà possibile per l'alunno recuperare i propri dati personali entro 30 giorni dalla cessazione del servizio. Successivamente l'indirizzo verrà sospeso per 3 mesi, quindi eliminato. b.

Per i docenti/personale ATA - Il servizio viene reso disponibile ai docenti per tutto il periodo di permanenza presso l'Istituto e cesserà con il termine del contratto, oppure qualora il docente venisse trasferito ad altro Istituto. Sarà possibile per il docente recuperare i propri dati personali

Documento di ePolicy - IC N. 9 - FORLI' - 19/06/2025 - 15:25 Pagina: 24/32
entro 3 mesi dalla cessazione del servizio. Successivamente l'indirizzo verrà sospeso per 3 mesi, quindi eliminato.

Art. 8

(Limiti di responsabilità dell'istituto)

a. L'istituto si avvale del servizio offerto dal fornitore Google Inc. con sede in 1600 Amphitheatre Parkway Mountain View, CA 94043, denominato "Google Suite for Education". Pertanto, l'istituto

non ha alcun potere per quanto concerne le misure necessarie a minimizzare il rischio di perdita d'informazioni e a garantire la riservatezza dei dati. Le politiche di gestione dei dati operate dal fornitore sono descritte nel sito ufficiale dello stesso.

b. L'utente solleva l'istituto da ogni responsabilità ed obbligazione in relazione alla cancellazione, al danneggiamento, o alla mancata conservazione dei contenuti nonché al mancato invio/ricezione di messaggi di posta (email).

c. Non sono previste attività di backup e di ripristino da parte dell'istituto dato che i server sono gestiti dal fornitore. L'utente provvederà per proprio conto alla realizzazione delle copie di sicurezza che ritenesse necessarie.

d. L'istituto si riserva la possibilità di sospendere temporaneamente o disattivare definitivamente il servizio.

Art. 9

(Riservatezza dei dati personali)

a. L'istituto si impegna ad utilizzare i dati relativi all'utente nel rispetto del Regolamento UE 679/2016

e del D.Lgs. 196/2003 e s.m.i., ai soli fini della creazione e mantenimento dell'account. aggiornato con le modifiche apportate, da ultimo, dalla L. 29 aprile 2024, n. 56.

b. Il servizio è erogato dal fornitore che applica la propria politica alla gestione della privacy; l'utente può conoscere in dettaglio tale politica visitando il sito web del fornitore come già specificato precedentemente.

Art. 10

(Infrazioni e sanzioni)

a. In caso di violazione delle norme stabilite nel presente Regolamento, l'Istituto, nella persona del suo rappresentante legale, il Dirigente Scolastico, e/o dell'Amministratore potrà sospendere

Documento di ePolicy - IC N. 9 - FORLI' - 19/06/2025 - 15:25 Pagina: 25/32
l'account dell'utente o revocarlo definitivamente senza alcun preavviso e senza alcun addebito a suo carico e fatta salva ogni altra azione di rivalsa nei confronti dei responsabili delle violazioni. b. Qualsiasi violazione del presente regolamento, di quelli di istituto nonché della legislazione vigente, connessa all'uso dell'account sarà sanzionata nelle modalità stabilite dai regolamenti dell'istituto.

c. L'Istituto si riserva la facoltà di segnalare alle autorità competenti - per gli opportuni accertamenti ed

i provvedimenti del caso - le eventuali violazioni alle condizioni di utilizzo indicate nel presente

Regolamento, oltre che alle leggi ed ai regolamenti vigenti.

3.3 - BYOD

La presente ePolicy conterrà indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device"). Risulta infatti fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Risulta importante per l'istituto dotarsi di un regolamento per l'uso dei dispositivi mobili a scuola (BYOD) che pertanto verrà redatto e implementato fra i documenti accessibili nel sito istituzionale.

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire). Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Queste, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.

Nelle procedure sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso, nonché le modalità di coinvolgimento del Dirigente Scolastico e del Referente per il contrasto al bullismo e al cyberbullismo. Inoltre, la scuola individua le figure che costituiranno un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica. La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

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

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

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenni e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Sexting: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere, per quanto possibile, la rimozione del materiale on-line e il blocco della sua diffusione per mezzo dei dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete.

Documento di ePolicy - IC N. 9 - FORLÌ - 19/06/2025 - 15:25 Pagina: 27/32

Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

Segnalazioni di eventi al referente del cyberbullismo via mail: eugeniatrotta@ic9forli.edu.it

4.2 - Quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale (ex [art. 357 c.p.](#)) in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

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

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

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

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

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

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

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

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo"

Documento di ePolicy - IC N. 9 - FORLI' - 19/06/2025 - 15:25 Pagina: 28/32
con l'obiettivo di allertare il Dirigente . La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso (valutare l'invio o meno della relazione agli organi giudiziari preposti) e agiscono tramite percorsi di sensibilizzazione.

CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe,

riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

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

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

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

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

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

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

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

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

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

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail

Documento di ePolicy - IC N. 9 - FORLI' - 19/06/2025 - 15:25 Pagina: 29/32

specifico per le segnalazioni; scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola; sportello di ascolto con professionisti; docente referente per le segnalazioni.

In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei

fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare e programmare percorsi di peer education per la prevenzione e il contrasto degli agiti.

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

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



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

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

Ricordare sempre che in base alla legge 71-2017:

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

Il DS (e/o il team antibullismo):

- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condivide informazioni e strategie.
- informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.

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

NELLE CLASSI

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

a seconda della situazione valuta se:

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

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

a) contenuto; b) modalità di diffusione.

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

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



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

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

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

Insieme si valuta se è il caso:

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

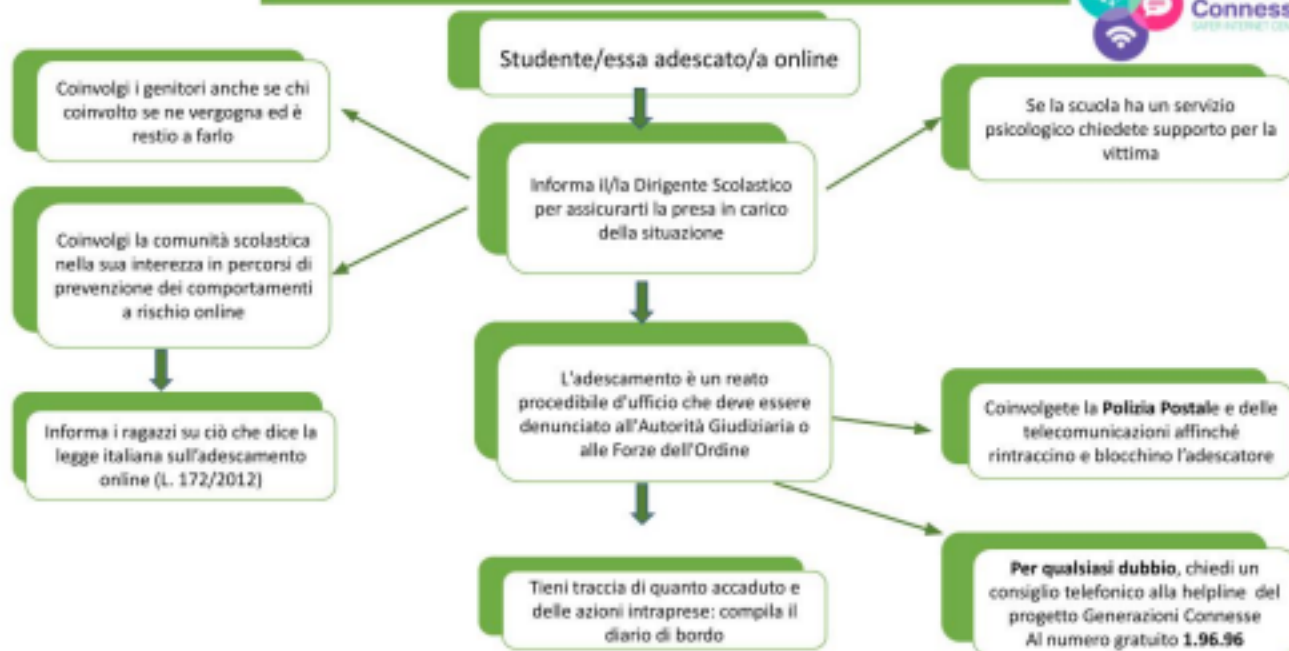
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

Se emergono evidenze passa allo schema successivo

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

Procedure interne: cosa fare in caso di Adescamento Online?



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

