



Ministero dell'Istruzione e del Merito

Istituto comprensivo statale "Ernesto Balducci" di Fiesole e Vaglia

IC "E. BALDUCCI"

Prot. 0018160 del 27/11/2025

II-1 (Entrata)

Fiesole, 14 novembre 2025

CONSIGLIO DI ISTITUTO del 14/11/2025 A.S. 2025 -2026

DELIBERA N. 82

OGGETTO: Approvazione documento ePolicy

VISTO il D.Lgs 297/94;

VISTA l'O.M. 215 del 15 luglio 1991;

VISTA l'O.M. n. 267 del 4 agosto 1995 e successive modifiche;

VISTO il documento ePolicy deliberato dal Collegio Docenti nella seduta del 12.11.2025

IL CONSIGLIO D'ISTITUTO DELIBERA il documento e Policy per l'Istituto Comprensivo "E. Balducci" Fiesole-Vaglia.

La delibera è assunta con voto palese all'unanimità.

Allegato documento ePolicy e schede sintetiche..

IL SEGRETARIO

Alessandra Rinaldi



Il 26/11/2025 alle 08:45:29,
Alessandra Rinaldi ha confermato
la volontà di apporre qui la propria
Firma Elettronica Avanzata ai sensi
dell'art. 20, comma 1-bis del CAD.

IL PRESIDENTE

Giulia Calzolari



Il 26/11/2025 alle 18:01:38,
Giulia Calzolari ha confermato
la volontà di apporre qui la propria
Firma Elettronica Avanzata ai sensi
dell'art. 20, comma 1-bis del CAD.

Avverso la presente delibera è ammesso reclamo al Consiglio d'Istituto ai sensi dell'art.14, 7° comma, del Regolamento n° 275/99 da chiunque vi abbia interesse, entro il 15° giorno dalla data di affissione all'Albo della scuola. Decorso tale termine la deliberazione è definitiva e contro di essa è esperibile ricorso giurisdizionale al T.A.R., ovvero ricorso straordinario al Capo dello Stato entro il termine rispettivamente di 60 e 120 giorni dalla data di pubblicazione.

Documento di ePolicy ERNESTO BALDUCCI

VIA DEL PELAGACCIO 1 - 50014 - FIESOLE

Firenze (FI) - Toscana

Data di approvazione: 23/10/2025 - 00:05

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.

Attraverso l'ePolicy, il nostro Istituto intende dotarsi di un documento di riferimento condiviso da tutta la comunità educante, volto a promuovere un uso consapevole, critico e responsabile delle tecnologie digitali. L'ePolicy rappresenta uno strumento operativo che orienta le azioni della scuola nell'ambito della cittadinanza digitale, favorendo la conoscenza delle opportunità e dei rischi legati all'utilizzo di Internet e delle TIC.

Essa definisce principi, regole e buone pratiche per garantire il benessere digitale e la sicurezza in Rete, ponendo le basi per percorsi di formazione, educazione e sensibilizzazione finalizzati a un uso corretto e positivo delle tecnologie nella vita scolastica e quotidiana.

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 DIRIGENTE SCOLASTICO

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 segue 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 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.

In merito all'organigramma dell'a.s. 25-26 si rimanda al documento allegato.

Il Collegio Docenti

- Promuove scelte didattiche ed educative orientate alla prevenzione dei comportamenti a rischio online e al contrasto dei fenomeni di prevaricazione, anche attraverso la collaborazione in rete con altre istituzioni scolastiche.

Il Consiglio di Classe

- Progetta e realizza attività didattiche e/o integrative che favoriscano il coinvolgimento attivo e collaborativo degli alunni e delle alunne, stimolando la riflessione sui valori della convivenza civile e della cittadinanza digitale.
- Si impegna a costruire un clima relazionale positivo e cooperativo all'interno della classe e nel rapporto con le famiglie, promuovendo iniziative e progetti di educazione alla legalità, al rispetto e alla cittadinanza attiva.

Il Direttore dei Servizi Generali e Amministrativi (DSGA)

- Vigila sulla corretta applicazione dell'ePolicy da parte del personale ATA.
- Propone eventuali modifiche o integrazioni al documento per migliorarne l'efficacia e l'attuazione.

Nel nostro Istituto non sono presenti i rappresentanti degli studenti e delle studentesse, in quanto scuola secondaria di I grado e quindi non sono presenti nel Team. Tra le figure facenti parte del Team vi è un rappresentante dei genitori in Consiglio di istituto (non il presidente).

Informativa per i soggetti esterni che operano nell'Istituto

Tutti coloro che, a vario titolo, svolgono attività educative o formative all'interno dell'Istituto devono:

- Mantenere sempre un comportamento coerente con il proprio ruolo educativo, improntato al rispetto, alla correttezza e alla professionalità.
- Agire nel rispetto del principio del superiore interesse del minore, ascoltando con attenzione e serietà le sue opinioni, esigenze e preoccupazioni.
- Astenersi da atteggiamenti o comportamenti irrispettosi, offensivi o lesivi della dignità, della privacy e dell'integrità personale degli studenti e delle studentesse.
- Non tollerare né partecipare a comportamenti illegali, abusivi o pericolosi per la sicurezza dei minori.

Tutti i soggetti esterni sono inoltre tenuti a conoscere e rispettare le norme interne dell'Istituto relative all'uso dei dispositivi digitali personali (smartphone, tablet, pc, ecc.) e di quelli scolastici, evitando qualsiasi uso improprio o non deontologicamente corretto durante le attività educative.

È fatto obbligo di tutelare la privacy dei minori, in particolare per quanto riguarda l'acquisizione e la diffusione di fotografie, immagini o video, nonché lo scambio di contatti personali (numeri telefonici, indirizzi e-mail, chat o profili social) come stabilito dal Patto di Corresponsabilità Educativa dell'Istituto.

Impegni dell'Istituto

L'Istituto predispone e diffonde un'informativa sintetica sull'ePolicy, comprensiva delle procedure di segnalazione, con l'obiettivo di:

- Rafforzare il rapporto di fiducia e collaborazione tra scuola e famiglie.
- Definire con chiarezza ruoli e responsabilità nei diversi ambiti di intervento.
- Attivare, quando necessario, le autorità competenti e i servizi territoriali, in un'ottica di prevenzione e di gestione condivisa dei casi rilevati.

È fondamentale garantire che tutti i soggetti esterni coinvolti nelle attività scolastiche siano adeguatamente formati e consapevoli dei rischi connessi all'uso delle tecnologie digitali e dei comportamenti corretti da adottare.

Le **organizzazioni, associazioni ed esperti esterni** che collaborano con l'Istituto nella realizzazione di progetti o attività educative sono tenuti a prendere visione dell'ePolicy e a **sottoscrivere un'apposita informativa sintetica** allegata al contratto di incarico, dichiarando di attenersi alle disposizioni in essa contenute.

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.

L'ePolicy è pienamente coerente con i principali documenti della nostra scuola, quali il RAV, il PTOF, il Regolamento d'Istituto (inclusivo del Regolamento per il bullismo e il cyberbullismo), il Regolamento di Disciplina, il Patto di Corresponsabilità Educativa, e la documentazione relativa alla privacy anche nel comparto Internet e uso delle TIC approvata dall'Istituto. Tutti questi documenti riportano specifici riferimenti alla sicurezza sul web, con particolare attenzione alla prevenzione e al contrasto del cyberbullismo.

Integrazione dell'ePolicy con i Regolamenti esistenti

L'ePolicy dell'Istituto si integra pienamente con i documenti normativi e regolamentari già in vigore, costituendo parte integrante del quadro educativo e organizzativo della scuola.

Il **Regolamento d'Istituto** e il **Patto di Corresponsabilità** verranno aggiornati con specifici riferimenti all'ePolicy, in coerenza con le **Linee Guida del MIUR** e con la normativa vigente in materia di cittadinanza digitale, tutela dei minori e uso consapevole delle tecnologie.

In particolare, l'ePolicy è conforme a quanto previsto da:

- **D.P.R. 24 giugno 1998 n. 249** - *Statuto delle studentesse e degli studenti della scuola secondaria*, come modificato dal **D.P.R. 21 novembre 2007 n. 235**;
- **Legge 29 maggio 2017 n. 71**, *Disposizioni a tutela dei minori per la prevenzione e il contrasto del cyberbullismo*, aggiornata dalla **Legge 17 maggio 2024 n. 70**, *Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e cyberbullismo* (in vigore dal 14 giugno 2024);

- **Legge 31 dicembre 1996 n. 675**, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, oggi confluita nel Regolamento UE 2016/679 (GDPR).

L'ePolicy, inoltre, si integra con gli obiettivi e i contenuti dei seguenti documenti d'Istituto:

- **PTOF**, comprensivo del piano per l'attuazione del **PNSD (Piano Nazionale Scuola Digitale)**;
- **Regolamento interno d'Istituto**;
- **Codice interno per il monitoraggio e il contrasto al bullismo e al cyber bullismo**
- **Curricolo Digitale d'Istituto**.

Gestione delle infrazioni all'ePolicy

Le eventuali violazioni delle disposizioni contenute nell'ePolicy saranno gestite in modo proporzionato alla gravità dei fatti, privilegiando sempre un approccio **educativo e formativo**.

In presenza di comportamenti più gravi, la scuola potrà prevedere **sanzioni disciplinari** nel rispetto del Regolamento d'Istituto e della normativa vigente.

L'Istituto promuove costantemente **iniziative di sensibilizzazione, formazione e prevenzione** per accrescere la consapevolezza degli studenti e delle studentesse sui rischi connessi all'uso delle TIC e della Rete, e per favorire un comportamento digitale responsabile.

In caso di episodi di particolare gravità, sarà cura della scuola **valutare l'opportunità di segnalazione alle autorità competenti** (ad esempio la Polizia Postale) e di attivare, ove necessario, forme di **supporto psicologico** o di mediazione, coinvolgendo i servizi territoriali competenti.

Disciplina degli alunni e delle alunne

Rientrano tra i comportamenti **sanzionabili o oggetto di intervento educativo**, in relazione all'uso improprio delle TIC, dei dispositivi digitali e della rete a scuola, le seguenti condotte:

- Utilizzo della rete per giudicare, offendere, denigrare o escludere altri, oppure per esprimersi in modo volgare o aggressivo.
- Condivisione incauta o non autorizzata di **foto, dati personali o informazioni sensibili** (es. indirizzo, numero di telefono).
- Pubblicazione o diffusione online di **immagini o video di compagni/e o del personale scolastico** senza consenso, in particolare se offensivi o denigratori.
- **Condivisione o invio di contenuti intimi o a sfondo sessuale**, propri o altrui.

- Invio di immagini o video finalizzati a **escludere o emarginare** altri studenti o studentesse.
- Comunicazione online **non autorizzata o imprudente con sconosciuti**.
- Accesso a **siti web non idonei o non indicati** dai docenti durante le attività didattiche o laboratoriali.

Tali condotte, oltre a costituire violazioni dell'ePolicy, rappresentano occasioni educative in cui la scuola si impegna a promuovere la **riflessione, la responsabilità personale e il rispetto delle regole di convivenza digitale** come tra l'altro stabilito nel Regolamento d'Istituto.

Ruolo e compiti del Dirigente Scolastico

Il **Dirigente Scolastico** svolge un ruolo centrale nell'attuazione e nel monitoraggio dell'ePolicy, garantendo la corretta gestione dei casi e la promozione di un ambiente digitale sicuro e responsabile. In particolare, egli:

- **Informa tempestivamente** e coinvolge le famiglie in caso di situazioni problematiche, **ad eccezione dei casi sospetti che richiedono la segnalazione diretta alle Forze dell'Ordine**.
- **Segnala ai Servizi Sociali del Comune e/o alla Tutela Minori** i casi in cui la famiglia non collabori o risulti inadeguata nella gestione della situazione.
- **Promuove e organizza attività di formazione e informazione** rivolte a tutta la comunità scolastica (personale, studenti, famiglie) per favorire la conoscenza e l'applicazione dell'ePolicy.
- **Raccoglie e documenta i fatti** attraverso l'apposita modulistica interna, presente nel Codice interno relativo al monitoraggio e al contrasto dei fenomeni di bullismo e cyber-bullismo, informando in tempi rapidi i genitori o i tutori legali degli studenti coinvolti.
- In presenza di **testimoni** e di un **genitore (in caso di minore)**, procede a:
 - **Ascoltare i protagonisti dei fatti** e i genitori per acquisire testimonianze e versioni complete dell'accaduto;
 - **Ricostruire gli eventi** sulla base delle informazioni raccolte;
 - **Accogliere e conservare eventuali documenti o materiali utili**, inclusi quelli consegnati da persone direttamente o indirettamente coinvolte.

Per ulteriori dettagli e approfondimenti, si rimanda alla sezione **"Regolamento d'Istituto"** del sito web scolastico, dove sono consultabili tutti i regolamenti dell'Istituto Comprensivo *E. Balducci*, compresi quelli relativi:

- alla **concessione e all'utilizzo dei dispositivi tecnologici**,
- al **Codice Interno per il contrasto dei fenomeni di bullismo e cyber-bullismo**

- alle **Netiquette** per un uso corretto e rispettoso delle piattaforme digitali,
- e all'**utilizzo della piattaforma Google Workspace for Education**.

Disciplina del personale scolastico

L'ePolicy stabilisce principi e regole di comportamento anche per il **personale scolastico**, al fine di garantire un utilizzo corretto, sicuro e professionale delle tecnologie digitali e di Internet.

Le eventuali infrazioni possono riguardare comportamenti o omissioni che incidono, direttamente o indirettamente, sulla sicurezza digitale, sulla tutela dei dati personali e sulla promozione di un uso consapevole delle TIC da parte degli studenti e delle studentesse.

Possibili infrazioni

Il personale scolastico, e in particolare i docenti, può incorrere in infrazioni relative a:

- **Uso improprio delle tecnologie o dei servizi digitali della scuola**, per finalità non attinenti all'attività didattica o al proprio profilo professionale, inclusa l'installazione di software non autorizzati o il salvataggio di materiali non idonei.
- **Comunicazioni elettroniche con genitori e/o alunni** non conformi al proprio ruolo istituzionale o ai principi di deontologia professionale.
- **Trattamento inadeguato dei dati personali o sensibili** degli studenti, in violazione delle norme sulla privacy o delle misure di sicurezza previste dal GDPR.
- **Diffusione o custodia non sicura delle credenziali di accesso (password)** o degli strumenti informatici assegnati, con il rischio che possano essere utilizzati da terzi.
- **Mancata o insufficiente vigilanza** durante le attività che prevedono l'uso delle TIC, tale da consentire comportamenti non autorizzati o incidenti.
- **Omissione della segnalazione** al Dirigente Scolastico, all'Animatore Digitale o al Team per l'Innovazione di episodi o criticità rilevanti.

Valutazione e gestione delle infrazioni

Le violazioni dell'ePolicy da parte del personale possono riguardare:

1. **L'uso improprio degli strumenti digitali e delle risorse informatiche dell'Istituto;**
2. **La mancata vigilanza o l'omissione di intervento** in caso di comportamenti scorretti da parte degli studenti.

La gravità dell'infrazione è valutata in base:

- al **livello di rischio o danno** procurato agli studenti e alla comunità scolastica;
- alla **tempestività e adeguatezza** delle azioni correttive intraprese.

Le misure conseguenti vengono gestite nel rispetto della **disciplina contrattuale** e delle **procedure previste dalla normativa vigente**.

Verifiche e controlli

Il **Dirigente Scolastico** può disporre verifiche sull'utilizzo delle TIC per accertarne la conformità alle regole di sicurezza e correttezza, incluse:

- la consultazione dei **log di accesso a Internet e alla posta elettronica** istituzionale;
- la **rimozione di materiali non pertinenti o non autorizzati** dai dispositivi o dai server scolastici, conservandone copia solo se necessario per eventuali approfondimenti o accertamenti successivi.

Tutto il personale è tenuto a **collaborare con il Dirigente Scolastico**, fornendo informazioni e supporto utili alla valutazione dei casi e all'avvio di eventuali procedimenti di natura **organizzativa, disciplinare, amministrativa o penale**, in relazione alla tipologia e alla gravità delle infrazioni.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curriculum 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 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.

Comunicazione e condivisione dell'ePolicy

Il documento di **ePolicy** è condiviso con l'intera **comunità educante**, ponendo al centro gli studenti e le studentesse e valorizzando il ruolo, i compiti e le responsabilità di ciascun soggetto coinvolto.

Ogni componente della scuola – docenti, personale ATA, studenti, genitori e figure di supporto – è chiamato a diventare **promotore attivo** dei principi e delle regole contenuti nell'ePolicy, affinché esse diventino patrimonio comune della cultura scolastica.

Strumenti e canali di condivisione

L'ePolicy viene comunicata e diffusa attraverso:

- **La pubblicazione sul sito istituzionale** della scuola, sia in versione integrale sia in formato sintetico e accessibile.
- **Il diario scolastico d'Istituto**, che riporta la versione *child friendly* del **Patto di Corresponsabilità**, ed eventualmente in una futura versione anche dei Documenti di E_Policy da sottoscrivere e restituire alle famiglie all'inizio dell'anno scolastico.

Gli studenti e le studentesse vengono informati del fatto che la loro attività online, all'interno degli spazi scolastici, è **monitorata e supportata** al fine di promuovere un uso sicuro e responsabile della rete.

All'inizio di ogni ciclo scolastico, l'ePolicy viene **presentata ai genitori e agli alunni** insieme al Patto di Corresponsabilità Educativa, in un'ottica di collaborazione tra scuola e famiglia.

Azioni e iniziative per la condivisione

L'Istituto Comprensivo E. Balducci di Fiesole e Vaglia promuove una serie di iniziative mirate per garantire una diffusione capillare e consapevole dell'ePolicy, differenziate in base ai destinatari.

Per i docenti

- Le **linee di condotta** relative alla sicurezza digitale vengono discusse negli **organi collegiali** e rese pubbliche attraverso il sito web della scuola.
- L'uso delle tecnologie digitali è **limitato alle finalità didattiche** e soggetto a controllo per garantire la sicurezza di personale e alunni.
- Il personale docente è informato del fatto che il **traffico Internet può essere monitorato** e riconducibile ai singoli utenti registrati.
- Il **sistema di filtraggio e monitoraggio** delle TIC è supervisionato dall'**Animatore Digitale**, che segnala eventuali criticità al Dirigente Scolastico o alla DSGA.
- L'Animatore Digitale mette a disposizione **strumenti e risorse digitali educative**, calibrate per età e competenze, utilizzabili dai docenti in classe.
- Tutto il personale è consapevole che eventuali **condotte non conformi al Codice di comportamento dei pubblici dipendenti** o ai doveri professionali possono comportare sanzioni disciplinari.
- I docenti ricevono **formazione e aggiornamento** sull'uso sicuro e responsabile delle tecnologie digitali, anche tramite materiali disponibili sul sito della scuola.
- In sede collegiale, è incoraggiata la **discussione e condivisione di buone pratiche** per integrare le tematiche dell'ePolicy nel curriculum e per elaborare **protocolli condivisi di intervento**.

Per gli studenti e le studentesse

- Lettura, comprensione e **sottoscrizione del Patto di Corresponsabilità**.
- Diffusione di un **estratto dell'ePolicy**, adattato all'età e al grado scolastico.
- Realizzazione di **lezioni dedicate** alle buone pratiche digitali, ai rischi della rete e alla prevenzione del cyberbullismo.
- Conoscenza e rispetto delle **regole d'uso dei laboratori informatici e dei dispositivi digitali**, con vigilanza da parte dei docenti.
- Ogni studente è **responsabile del dispositivo** assegnato; eventuali violazioni sono sanzionate secondo il

Regolamento d'Istituto.

Per i genitori

- Lettura e comprensione del **Regolamento d'Istituto** e sottoscrizione del **Patto di Corresponsabilità**.
- Partecipazione a **incontri informativi e formativi** per promuovere un approccio condiviso alla sicurezza digitale.
- L'**Animatore Digitale** fornisce **materiali informativi e risorse online** per favorire un uso consapevole e sicuro di Internet in famiglia.
- I docenti forniscono **riferimenti a siti e risorse educative** utili per lo studio e la crescita digitale degli studenti.

Comunicazione inclusiva e differenziata

Nella diffusione dell'ePolicy, l'Istituto considera i diversi **destinatari** (alunni, docenti, genitori, personale ATA, collaboratori scolastici) e adotta **linguaggi, modalità e canali di comunicazione diversificati**, definiti progressivamente in base alle esigenze.

È prevista anche la redazione di una **versione "child friendly"** del documento, accessibile e comprensibile per i più giovani.

Approvazione e inserimento nel PTOF

L'ePolicy è **redatta dal Team Antibullismo e dell'Emergenza e dal Team Innovazione, approvata dal Collegio Docenti e dal Consiglio di Istituto**, e successivamente **inserita nel PTOF**, a testimonianza della sua piena integrazione nella progettazione educativa e digitale dell'Istituto Comprensivo E. Balducci di Fiesole e Vaglia.

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.

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.

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

Monitoraggio, revisione e aggiornamento dell'ePolicy

L'ePolicy è un documento dinamico, soggetto a **monitoraggio e aggiornamento periodico**, al fine di garantirne la coerenza con l'evoluzione delle tecnologie digitali, delle normative vigenti e delle pratiche educative dell'Istituto.

L'aggiornamento avviene:

- **con cadenza periodica** o ogniqualvolta si verifichino **cambiamenti significativi** nell'utilizzo delle tecnologie digitali nella scuola;
- in occasione di **modifiche normative** o dell'emergere di **nuove esigenze educative e organizzative**;
- in concomitanza con la stesura o la revisione del **Rapporto di Autovalutazione (RAV)**, sulla base dei casi problematici riscontrati e delle modalità di gestione attuate.

Le **modifiche e integrazioni** dell'ePolicy vengono discusse e condivise con tutto il **personale docente** e, se necessario, con gli altri membri della comunità scolastica, in un'ottica di partecipazione e corresponsabilità.

Il **monitoraggio dell'efficacia del documento** viene realizzato attraverso la valutazione del raggiungimento degli **obiettivi specifici** e l'analisi dei risultati ottenuti in termini di prevenzione, sicurezza digitale e promozione del benessere online.

Il **Gruppo di Lavoro per l'ePolicy** – composto dai referenti che ne hanno curato la redazione – è responsabile delle attività di **monitoraggio, revisione, aggiornamento e implementazione** del documento, assicurandone la costante attualità e coerenza con le linee strategiche dell'Istituto.

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.

I ragazzi utilizzano quotidianamente la Rete, spesso in modo più naturale e veloce rispetto agli adulti, ma questo non significa che abbiano automaticamente competenze digitali avanzate. La competenza digitale richiede interesse e capacità di usare le tecnologie con sicurezza, spirito critico e responsabilità, includendo alfabetizzazione informatica, comunicazione e collaborazione online, creazione di contenuti, sicurezza digitale, conoscenza della proprietà intellettuale e pensiero critico. Per questo la scuola promuove percorsi educativi mirati a sviluppare queste abilità, favorendo un utilizzo consapevole e responsabile delle tecnologie attraverso un curriculum digitale strutturato.

2.2 - Il Curriculum 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.

In questo contesto, l'Istituto Ernesto Balducci di Fiesole e di Vaglia, nell'ambito del miglioramento della propria offerta formativa, ha già predisposto un curriculum digitale, attualmente in fase di bozza e di elaborazione, la cui approvazione ufficiale è prevista nella prima parte dell'anno scolastico.

Il presente documento si basa sul DigComp 2.2 (Vuorikari, Kluzer e Punie). L'Istituto si impegna a promuovere negli insegnamenti disciplinari lo sviluppo delle competenze digitali, seguendo i descrittori e i livelli di apprendimento indicati.

La definizione delle competenze digitali e dei relativi livelli di apprendimento richiede l'adozione di metodologie didattiche innovative che favoriscano la partecipazione attiva degli studenti e delle studentesse. In tale prospettiva, la ricerca, la collaborazione, la comunicazione e la produzione digitale costituiscono ambiti di apprendimento privilegiati, promuovendo lo sviluppo di capacità personali e relazionali (soft skills) e sostenendo l'educazione al lifelong learning.

Il raggiungimento degli obiettivi del Curriculum Digitale avviene mediante l'uso combinato di strumenti didattici e attrezzature digitali. Le metodologie innovative, integrate con le tecnologie digitali, consentono di potenziare abilità e competenze, promuovere l'inclusione e garantire esperienze di apprendimento significative e personalizzate.

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 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.

È essenziale che tutti i docenti siano adeguatamente formati e aggiornati sull'uso corretto ed efficace delle TIC nella didattica, al fine di impiegarle in modo integrativo e inclusivo. Ciò consente di offrire agli studenti modelli positivi e critici di utilizzo delle tecnologie e di armonizzare gli apprendimenti.

La complessità della professione docente richiede competenze diverse e integrate, tra cui quelle digitali, necessarie per progettare, sviluppare, gestire e valutare i processi di insegnamento e apprendimento per tutti gli alunni. La competenza digitale rappresenta oggi un requisito imprescindibile, poiché consente di diversificare e innovare la didattica, adattandola ai nuovi stili di apprendimento.

Attualmente, solo un numero limitato di docenti dell'Istituto ha familiarità con il Kit Didattico. Risulta quindi prioritario presentarlo a tutto il corpo docente e favorirne l'inserimento graduale nelle attività didattiche finalizzate all'uso consapevole e corretto di Internet.

L'Istituto, pertanto, promuove e sostiene la partecipazione del personale a iniziative formative organizzate dalla scuola, dalle reti di istituti, dall'amministrazione o autonomamente dai docenti, anche in modalità online.

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 scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino". (cfr. <https://www.garanteprivacy.it/temi/scuola>).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il "corretto trattamento dei dati personali" a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore il 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente

ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali. Tali documenti sono reperibili sul sito della scuola: <https://www.comprensivofiesole.edu.it> nella sezione **Scuola - Le carte della scuola - Privacy**.

L'Istituto ospita alunni/e dai 3 ai 14 anni, per questo è fondamentale fare tutto il possibile per evitare che siano esposti a contenuti inappropriati. In fase di iscrizione degli alunni/e alla scuola i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza all'art. 13 D.Lgs 30 giugno 2003, n. 196 modificato dal D.Lgs 101 del 2018 (Codice in materia di protezione dei dati personali).

Al momento dell'iscrizione i genitori rilasciano il consenso all'utilizzo di materiale fotografico e audiovisivo e all'esposizione degli elaborati degli alunni/e anche in sedi diverse da quelle dell'Istituto. I dati sensibili sono a esclusivo uso della dirigenza e della segreteria. I computer che contengono queste informazioni sono protetti da un ingresso con nome utente e password noti solo al personale preposto.

L'accesso ai dati riportati nel Registro Elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori dell'Istituto, tramite l'invio di una password di accesso strettamente personale.

All'interno dell'istituzione scolastica, il responsabile della gestione del trattamento dei dati personali è il Dirigente Scolastico, il quale indica nella persona del DSGA e nel personale amministrativo gli incaricati al trattamento dei dati.

La segreteria utilizza password nelle postazioni informatiche di lavoro, individua soggetti preposti alla gestione delle password, ha un codice identificativo personale per ogni utente, utilizza programmi antivirus, protegge e regola gli accessi locali che ospitano le informazioni riservate o in cui si trovano le postazioni di lavoro che ne consentono l'accesso, definisce i criteri per garantire l'integrità e la trasmissione sicura dei dati e si dota di mezzi elettronici adeguati per impedire l'accesso dall'esterno alla propria rete.

Le fotografie e i video da pubblicare sul sito che includano gli alunni/e sono selezionati con cura e non permettono l'identificazione dei singoli attraverso l'indicazione del nome, a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione.

Nella Guida del Garante per la protezione dei dati personali "La scuola a prova di privacy" sono specificate le linee guida da seguire riguardo il trattamento dei dati personali all'interno della comunità scolastica. Tutte le scuole hanno l'obbligo di far conoscere agli alunni/e, alle famiglie e ai docenti le modalità di trattamento dei loro dati personali. Ogni persona ha diritto di conoscere se sono conservate informazioni che la riguardano, di apprendere il contenuto, di farle rettificare se erranee, incomplete o non aggiornate. Per esercitare questi diritti è possibile rivolgersi direttamente al "titolare del trattamento", anche tramite i suoi incaricati o responsabili del trattamento dei dati. Se non si ottiene risposta o se il riscontro non risulta adeguato è possibile rivolgersi al Garante o alla magistratura ordinaria.

L'accesso agli atti è regolato dall'amministrazione che deve valutare l'esistenza di presupposti normativi che permettano la presa visione o estratto/copia conforme dei documenti ai soggetti con un "interesse diretto, concreto e attuale" alla conoscibilità degli atti.

L'utilizzo del telefono cellulare e di apparecchi per la registrazione di suoni e immagini è disciplinato dal Regolamento di Istituto pubblicato sul sito della scuola. Nessun membro della comunità scolastica, in alcuna occasione (ad esempio, all'interno della scuola o durante un'uscita didattica), può diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su internet).

Le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici non violano la privacy. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare e non alla diffusione. Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su internet. In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso scritto informato delle persone presenti nelle fotografie e nei video dei genitori (o di chi ne fa le veci) nel caso di minori.

Le scuole di ogni ordine e grado sono soggette a un regime di pubblicità e trasparenza. L'Istituto scolastico presta particolare attenzione a non rendere accessibili informazioni che dovrebbero restare riservate o a mantenerle online oltre il tempo consentito.

Inoltre, la scuola non ha solo il compito di tutelare la privacy degli alunni/e e delle loro famiglie, ma anche quello di informare e rendere consapevoli gli alunni/e di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

Cosa sono i "dati personali"

I dati personali sono tutte quelle informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc. Fra questi, particolarmente importanti sono:

- i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- i dati che permettono l'identificazione indiretta di una persona, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, ...);
- i dati sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale e dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- i dati giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti a iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitiva, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) comprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
- altri dati personali che hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via internet o telefono) e quelli che consentono la geo-localizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti di una persona.

I protagonisti dei "dati personali"

- L'interessato è la persona fisica alla quale si riferiscono i dati personali (art. 4, paragrafo 1, punto 1 del Regolamento UE 2016/679);
- il titolare è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico, privato o l'associazione che adotta le decisioni sugli scopi e sulle modalità del trattamento (art. 4, paragrafo 1, punto 7 del Regolamento UE 2016/679);
- il responsabile è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati (art. 4, paragrafo 1, punto 8 del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. sub-responsabile (art. 28, paragrafo 2).

Il trattamento dei "dati personali"

Trattamento è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali. Ad esempio: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, par. 1, punto 2, del Regolamento (UE) 2016/679).

I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantire il corretto

e sicuro utilizzo dei dati.

Gli obblighi delle scuole in merito alla protezione dei "dati personali"

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore.

In caso di violazione del trattamento dei dati la persona interessata può presentare al Garante per la Protezione dei dati personali un'apposita "segnalazione" gratuita o un "reclamo" (più circostanziato rispetto alla semplice segnalazione e con pagamento di diritti di segreteria).

Le scuole, sia pubbliche che private, hanno l'obbligo di informare tramite apposita informativa gli interessati delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Gli interessati non sono solo gli alunni/e, ma anche le famiglie e gli stessi docenti. È importante, inoltre, che le scuole verifichino i loro trattamenti, controllando se i dati siano eccedenti rispetto alle finalità perseguite.

Nel 2016 il Garante per la protezione dei dati personali ha pubblicato un utile vademecum "La scuola a prova di privacy" che offre agli insegnanti e ai dirigenti una guida per gestire correttamente le questioni legate alla diffusione e al trattamento dei dati personali degli alunni/e e delle famiglie. Il documento è stato elaborato prima dell'applicazione del Regolamento UE 679/2016, avvenuta il 25 maggio 2018, ma rimane un riferimento molto utile per aiutare docenti, famiglie, alunni/e e la stessa amministrazione scolastica a muoversi più agevolmente nel delicato mondo della protezione dei dati personali.

La liberatoria

La scuola non è tenuta a richiedere alle famiglie l'autorizzazione alle riprese fotografiche e video (ad es. in caso di gite scolastiche o recite) solo se esse sono realizzate a fini personali e non a fini di pubblicazione o divulgazione. Famiglie e alunni/e hanno il diritto di conoscere quali informazioni sono trattate dall'Istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

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.

Accesso a Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*

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

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet (27 ottobre 2014), inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

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

Infrastruttura tecnologica dell'Istituto

La scuola è presente sulla rete con un portale web: www.comprensivofiesole.edu.it costantemente aggiornato contenente le informazioni utili per il personale scolastico e per le famiglie.

In ottemperanza alle leggi tutti i plessi dell'Istituto Comprensivo "E. Balducci" di Fiesole e Vaglia sono dotati di accesso alla Rete internet tramite wifi, rete protetta da password. E' possibile accedere alla rete da tutti i dispositivi digitali scolastici. I docenti e il personale ATA possono accedere alla rete anche con i propri dispositivi personali facendo richiesta della password di accesso al Referente informatico di plesso. L'accesso a internet degli alunni/e è ammesso in presenza del/i docente/i ed esclusivamente per motivi didattici. L'accesso è per tutti schermato da filtri che dal server impediscono il collegamento a siti appartenenti a black list o consentono il collegamento solo a siti idonei alla didattica, secondo le impostazioni date dall'amministrazione che periodicamente provvede alla manutenzione e aggiornamento del sistema informatico di Istituto, ove necessario richiedendo l'intervento di tecnici esterni.

Tutte le classi, laboratori, corridoi e spazi comuni sono dotati di accesso internet, di una rete wi-fi sufficientemente adeguata al numero di alunni/e, in grado di supportare il traffico dati generato da un numero elevato di utenti e permettere, ad esempio, l'uso di soluzioni cloud per la didattica e l'uso di contenuti di apprendimento multimediali.

Opportunità rese tali dal monitoraggio costante avvenuto negli anni, dalla partecipazione a bandi PON o europei, ma anche dalla collaborazione con le amministrazioni locali dei Comuni di Fiesole e Vaglia.

Tutte le classi delle scuole primarie e secondarie sono dotate di monitor e hanno a disposizione un certo numero di iPad per creare laboratori e attuare attività in classe. I tablet sono gestiti tramite la piattaforma Jamf e messi in sicurezza tramite Radar di Jamf.

I plessi delle scuole dell'infanzia sono dotati di Lim.

Al momento, sono presenti due laboratori d'informatica: nel plesso di Pratolino a disposizione della scuola primaria e secondaria e nel plesso della scuola primaria "L. Casini" di Pian di Mugnone.

In tutti i plessi dell'Istituto, dall'infanzia alla secondaria, sono disponibili piccoli robot: Cubetto, Blue Bot, Kai's Clan, ecc.

L'Istituto utilizza il Registro Elettronico al quale i docenti, gli alunni/e, i genitori accedono con credenziali personali, la piattaforma Google Workspace for Education tramite account istituzionale (.....@comprensivofiesole.edu.it) e tutte le altre piattaforme in uso nell'Istituto. In essi è consentito caricare materiale didattico e scambiare messaggi tra docenti e alunni/e e tra docenti e famiglie, ma il loro utilizzo è vincolato al possesso delle credenziali fornite dalla scuola e all'utilizzo della posta istituzionale.

I docenti e gli ATA hanno la mail nome.cognome@comprensivofiesole.edu.it, le cui credenziali vengono consegnate al momento della presa di servizio.

A fine contratto, per termine della supplenza, vengono dati ulteriori 15 giorni per il salvataggio dei propri documenti, mentre per coloro che hanno ottenuto il trasferimento o il pensionamento, la mail verrà cancellata il 31 agosto. Per coloro che hanno avuto l'assegnazione provvisoria, la mail viene sospesa.

Gli studenti hanno la mail cognome.nome@comprensivofiesole.edu.it, previa compilazione e consegna del modulo di consenso firmato dai genitori. La fruibilità del servizio è limitata al dominio comprensivofiesole.edu.it, pertanto essi potranno comunicare via mail e condividere materiali solo con i membri interni all'Organizzazione.

La mail ha durata triennale per i ragazzi della scuola secondaria di primo grado.

Viene creata il primo anno di frequenza e viene cancellata al termine. I docenti affiancano i ragazzi nell'accesso alla mail e nella salvaguardia della password.

La piattaforma *Google workspace for Education*, non include annunci promozionali, non utilizza mai i contenuti o i dati degli studenti a fini pubblicitari. Essa inoltre ha un valore fortemente inclusivo, in quanto consente agli studenti di imparare a lavorare in modo collaborativo e condiviso.

Un ambiente sicuro anche online

In inglese esistono due termini per parlare di sicurezza:

- “safety”: riguarda la prevenzione dei rischi, a partire dalla consapevolezza, conoscenza e preparazione per un uso consapevole delle tecnologie digitali (è questo l'approccio del progetto “Generazioni Connesse”);
- “security” che, in relazione a internet e ai media, si riferisce a tutte quelle risorse tecnologiche che rendono sicuro l'ambiente digitale, dall'antivirus al firewall, da un protocollo di trasmissione dei dati sicuro (https) all'aggiornamento di software e sistemi operativi.

Il nostro Istituto Scolastico considera l'ambiente online alla stregua dell'ambiente fisico e ne valuta, quanto più possibile, tutti gli aspetti legati alla sicurezza.

In riferimento alla security, si presta attenzione non solo all'infrastruttura hardware e alla rete (wireless e non), ma si considera anche:

- la sicurezza di tutti gli aspetti che riguardano la gestione degli account degli utenti (in modo differenziato tra

alunni/e, insegnanti, personale scolastico/amministrativo);

- il filtraggio dei contenuti e gli aspetti legali in relazione prevalentemente alla privacy. L'accesso alla rete è protetto da apposito Firewall e l'Istituto conserva i log di accesso che verranno forniti, in caso di richiesta, alle Forze dell'Ordine.

Sono presenti reti separate per la segreteria e per la didattica. Le reti non comunicano tra loro al fine di garantire la riservatezza dei dati di segreteria.

Interventi tecnici

La scuola provvede a pianificare interventi periodici di manutenzione, segnalando eventuali problematiche riscontrate ai Referenti informatici di plesso e/o al Team Digitale, i quali provvedono tempestivamente a porre rimedio formando sul campo i docenti in difficoltà, permettendo loro, qualora le problematiche si ripresentino, di affrontare e risolvere in autonomia tutte quelle situazioni e casistiche di malfunzionamento dei dispositivi che si possono presentare nella quotidianità.

Le operazioni di gestione, configurazione, backup e ripristino sono affidate all'Animatore Digitale e alla risorsa tecnica interna presente, in maniera saltuaria, nell'Istituto, affiancate dalla ditta esterna di supporto.

Il regolamento sull'uso delle tecnologie a scuola

L'accompagnamento da parte degli adulti è fondamentale nel percorso di crescita degli alunni per aiutarli a sviluppare le competenze digitali necessarie alla convivenza civile e al futuro lavorativo di alunni/e.

Il personale scolastico è tenuto a seguire le seguenti regole di accesso a internet:

- è possibile accedere a internet attraverso strumentazioni in dotazione all'Istituto;
- l'accesso a internet e la navigazione attraverso le strumentazioni scolastiche è riservato a un uso strettamente didattico;
- è possibile accedere ad account personali durante l'uso di internet, ma è obbligatorio il logout al termine;
- non è consentito il salvataggio di dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche;
- è vietato scaricare o installare da internet materiale potenzialmente dannoso, di provenienza non sicura o non legale.

Gli alunni/e sono tenuti a rispettare le seguenti regole di accesso a internet:

- è vietato l'accesso a internet senza autorizzazione da parte del personale docente;
- è vietata la navigazione in assenza del docente;
- l'accesso a internet e la navigazione attraverso le strumentazioni scolastiche è riservato a un uso strettamente didattico e nel rispetto di diritti della cittadinanza digitale e delle norme vigenti di utilizzo legale della rete;
- è vietato il salvataggio di dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche;

- è vietato scaricare da internet materiale senza l'autorizzazione del docente.

Tutti gli operatori presenti a qualsiasi titolo nella scuola (esperti esterni, collaboratori, ditte esterne...) dovranno attenersi alle regole generali previste per il personale.

Checklist per la cybersecurity

- Reti separate di didattica e segreteria: importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le reti grazie al firewall.
- Aggiornamento periodico di software e Sistema Operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- Programmazione di backup periodici: copiare e mettere in sicurezza i dati del sistema scolastico per prevenire la perdita degli stessi.
- Formazione adeguata al personale scolastico: la formazione deve riguardare in particolare la gestione dei dispositivi e la conoscenza delle regole basilari sulla sicurezza.
- Disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo: prevedere l'accesso ai dispositivi tramite inserimento di password, anche in seguito a stand-by, per evitare il rischio potenziale di accesso da parte di persone non autorizzate.
- Indicazioni sulle password:
 - o sensibilizzare rispetto all'uso di password difficilmente identificabili;
 - o non memorizzare le password nei dispositivi scolastici;
 - o non condividere le password con nessuno.

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.

Strumenti di comunicazione online

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

I dispositivi digitali dell'Istituto sono monitorati e tenuti aggiornati dai docenti di riferimento affiancati da tecnici

esterni specializzati.

In tutti i plessi è stato attivato un firewall di Istituto per bloccare l'accesso a siti e contenuti inappropriati per il contesto scolastico.

La connessione alla rete wi-fi d'Istituto è accessibile solo in seguito all'inserimento di una password comune.

I dispositivi digitali a disposizione degli insegnanti sono protetti da password di accesso, a tutela dei dati sensibili, mentre i computer destinati agli alunni/e sono privi di password e vengono utilizzati esclusivamente sotto la supervisione di un insegnante. Nei dispositivi degli studenti non è visibile la password alla wifi.

Strumenti di comunicazione online utilizzati a scuola

Fra gli strumenti di comunicazione troviamo:

1. il sito web della scuola raggiungibile all'indirizzo (www.comprensivofiesole.edu.it), utilizzato per fornire informazioni di servizio rivolte ad alunni/e e genitori a integrazione delle comunicazioni, circolari e avvisi trasmessi mediante il Registro Elettronico e per trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che l'Istituto porta avanti;
2. il Registro Elettronico con tutte le sue funzionalità: utilizzato per facilitare e rendere più partecipata la didattica e la comunicazione scuola-famiglia;
3. la piattaforma Google Workspace for Education, con le sue app incluse: e-mail, drive, meet, classroom, etc. A ogni docente e alunno/a di scuola secondaria di I grado è assegnato un indirizzo e-mail istituzionale (.....@comprensivofiesole.edu.it) utilizzato per scopi didattici.

La sicurezza e la privacy, nonché le prerogative di accesso, sono garantite mediante password individuali, generate da un'apposita procedura interna e comunicate ai destinatari a mezzo posta elettronica o cartacea, in presenza.

Ogni utente è responsabile delle proprie credenziali (username e password); in caso di smarrimento o dimenticanza è necessario contattare l'amministratore della GSuite.

Si sollecita la custodia responsabile di tutte le credenziali personali.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne è importante ricordare quello che si può definire "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione tra vita lavorativa e vita familiare.

Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

Per ciò che concerne la gestione degli strumenti personali (cellulari, tablet, pc) da parte di alunni/e, docenti, personale scolastico e ogni altro operatore presente a qualsiasi titolo nella scuola si fa riferimento a quanto riportato nel Patto di Corresponsabilità, nei Regolamenti di Istituto e alla normativa di riferimento rappresentata dalla Circolare Ministeriale n.

3392 del 16/06/2025, che estende il divieto dell'uso di cellulari a scuola anche alle scuole secondarie di secondo grado, e dalla Nota Ministeriale n. 5274 dell'11 luglio 2024, che ha introdotto le nuove disposizioni.

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 minorenne 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.

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.

Il nostro Istituto ha formato un Team composto dal Dirigente Scolastico e quattro docenti referenti per il bullismo e cyberbullismo, uno per ogni plesso della scuola Secondaria e uno per la scuola Primaria, che si occupano di sostenere gli altri docenti nelle attività di prevenzione, monitoraggio e contrasto.

I docenti del Team hanno seguito un percorso di formazione specifico su varie piattaforme, Piattaforma Elisa e Generazioni Connesse.

L'Istituto ha adottato un codice interno per la prevenzione e il contrasto del bullismo e cyberbullismo e un protocollo di intervento.

Tale documento comprende: definizioni di bullismo e cyberbullismo, le differenze tra i due, i soggetti coinvolti, le conseguenze del bullismo e cyberbullismo, i riferimenti normativi, i soggetti coinvolti e i vari ruoli, i ruoli e le azioni di contrasto al bullismo e cyberbullismo, la prevenzione primaria, secondaria e terziaria, le azioni di intervento nei casi di bullismo e cyberbullismo. Nel documento sono inserite anche le schede di prima segnalazione dei casi di bullismo e cyberbullismo la scheda di monitoraggio degli episodi di bullismo e cyberbullismo e di valutazione della prevenzione (vedi il documento in allegato).

L'Istituto "E.Balducci" vuole sensibilizzare e prevenire i fenomeni del bullismo e cyberbullismo attraverso:

- azioni a livello individuale come la conoscenza del fenomeno, miglioramento delle competenze digitali, potenziamento dell'autostima di ciascuno
 - azioni a livello della classe come conoscenza del fenomeni del bullismo e cyberbullismo, la promozione della conoscenza reciproca, la coesione, il rispetto e la risoluzione dei conflitti
 - azioni a livello d'Istituto come la nomina di un Team per il bullismo e cyberbullismo, corsi di formazione per tutti gli insegnanti, l' istituzione di una giornata dedicata alla sensibilizzazione degli alunni su queste tematiche, uno sportello d'ascolto psicologico e la consulenza di uno psicologo.
- Le azioni di contrasto dei fenomeni del bullismo e cyberbullismo si svolgono a livello individuale e della classe attraverso la rilevazione del fenomeno con questionari, la discussione e condivisione dei dati raccolti nei Consigli di Classe per individuare strategie efficaci. Il Team discute i casi raccolti e mette in campo una strategia di intervento, l'Istituto ha adottato un regolamento che disciplina l'utilizzo dei cellulari all'interno della scuola.

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" 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 minorenni.

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

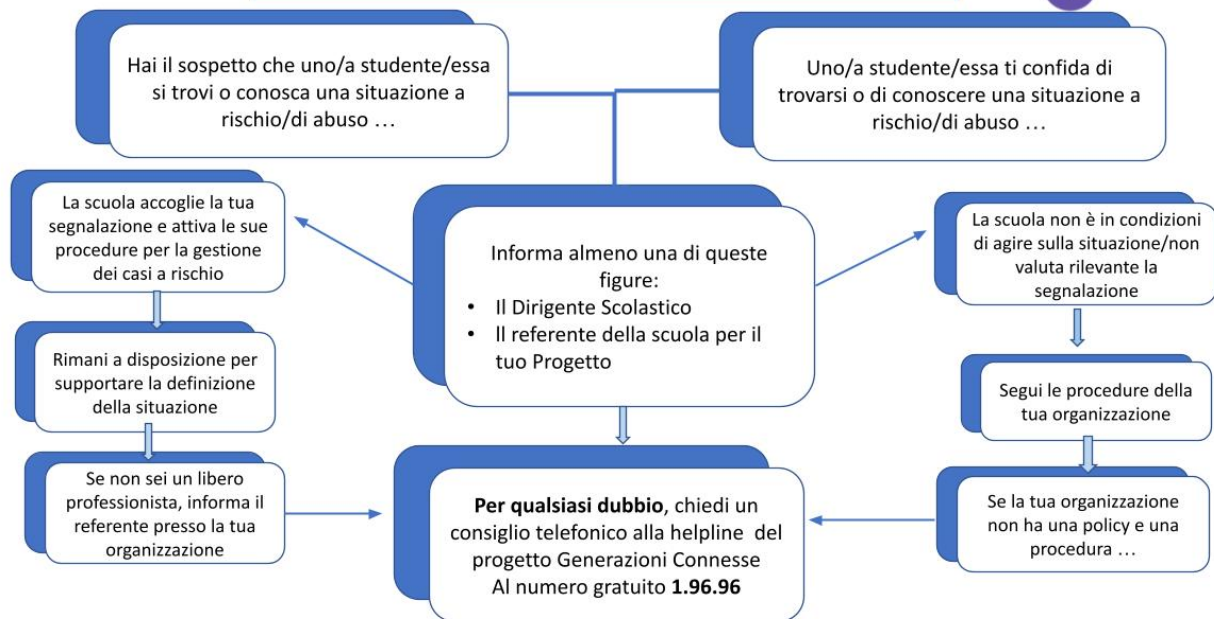
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

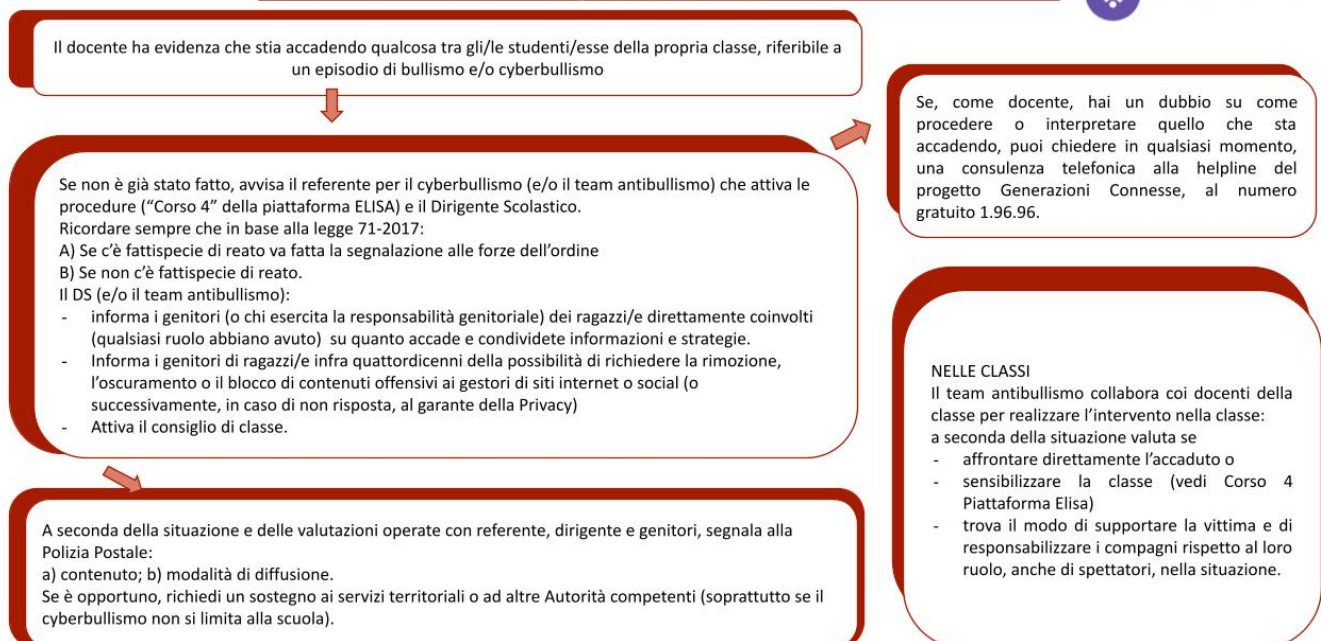
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle [Linee di Orientamento per la prevenzione e il contrasto 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 di segnalazione per enti, associazioni, professionisti esterni alla scuola



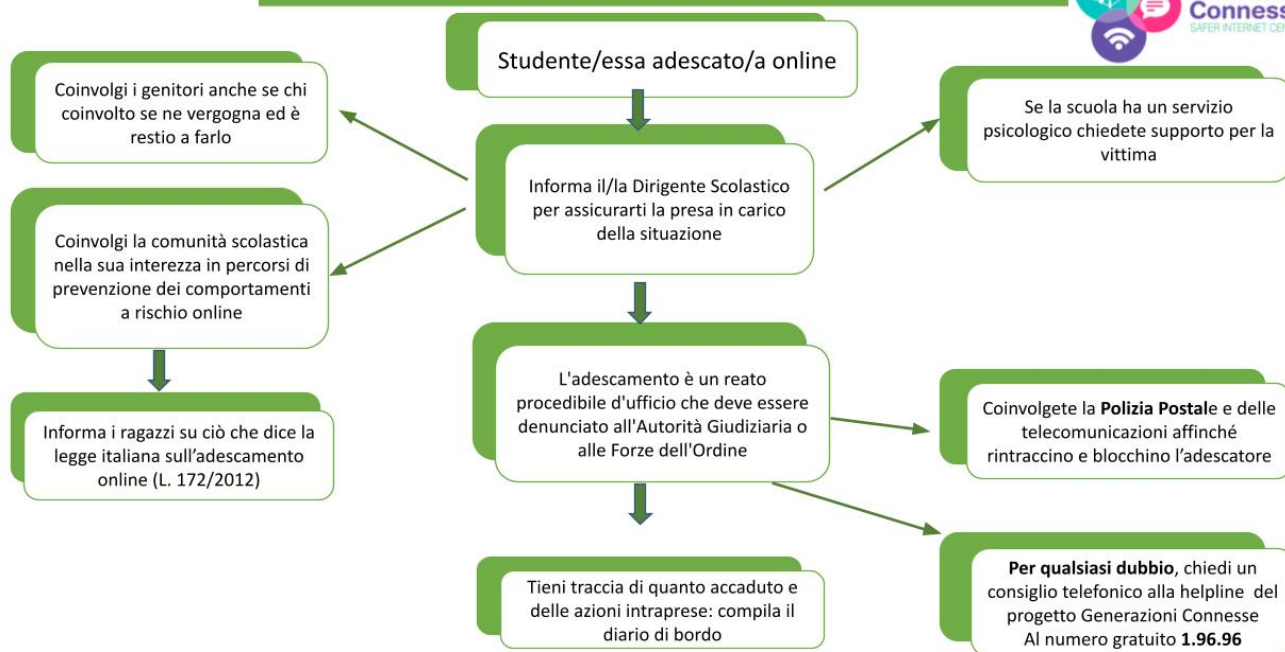
Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

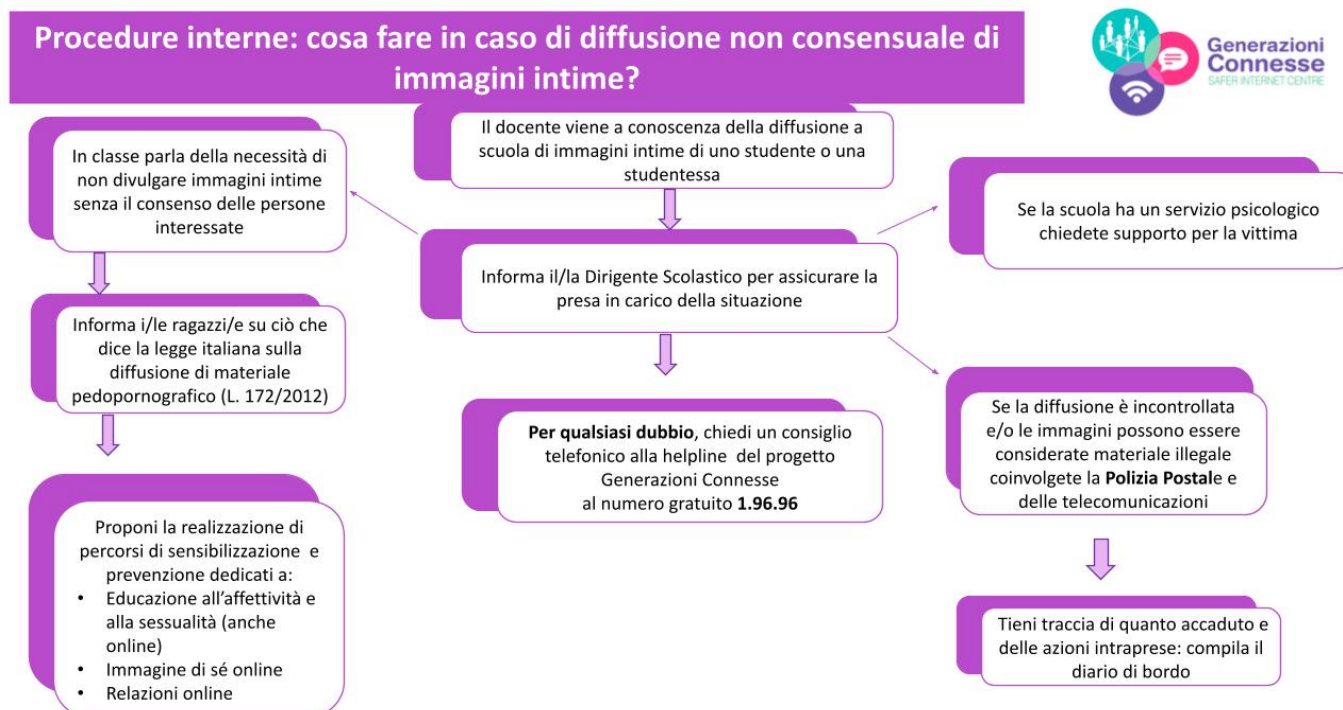


Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Procedure interne: cosa fare in caso di Adescamento Online?





L'Istituto "E.Balducci" di Fiesole ha elaborato un codice interno per la prevenzione, il contrasto e la gestione dei fenomeni del bullismo e cyberbullismo. A tale scopo ha formato un Team composto dal Dirigente scolastico e quattro referenti, uno per ogni plesso della scuola Secondaria e uno per la scuola Primaria. Il Team, durante lo scorso anno scolastico, ha diffuso delle iniziative formative su bullismo e cyberbullismo.

Per quanto riguarda la gestione dei casi in emergenza e in monitoraggio si rimanda al codice interno precedentemente citato.



Ministero dell'Istruzione e del Merito

Istituto comprensivo statale “ Ernesto Balducci” di Fiesole eVaglia

Documento Sintetico dell'ePolicy dell'Istituto E. Balducci di Fiesole e Vaglia per Studenti e Studentesse
(Approvato il 23/10/2025)

Agli studenti e alle studentesse dell'Istituto E. Balducci di Fiesole e Vaglia

Questo documento riassume le regole fondamentali dell'ePolicy del nostro Istituto, un piano che ha come obiettivo principale quello di promuovere in te una **competenza digitale positiva, critica e consapevole** nell'uso delle tecnologie.

L'ePolicy è il documento di riferimento per garantire il tuo **benessere digitale e la sicurezza in Rete**, assicurando un uso responsabile e positivo della rete.

1. Il Tuo Ruolo e le Tue Responsabilità

Sei una parte fondamentale della comunità educante e hai compiti precisi nell'applicazione dell'ePolicy:

1. **Uso consapevole:** Devi utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti, in base al tuo grado di maturità e consapevolezza.
2. **Protezione:** Con il supporto della scuola, devi imparare a tutelare te stesso/a e i tuoi/le tue compagni/e, rispettandoli/le online.
3. **Partecipazione:** Sei chiamato/a a partecipare attivamente a progetti e attività che riguardano l'uso positivo delle Tecnologie dell'Informazione e della Comunicazione (TIC) e della Rete, e puoi farti promotore di queste conoscenze (ad esempio, tramite la *peer education*).
4. **Informazione:** Sappi che l'ePolicy viene presentata a te e ai tuoi genitori insieme al Patto di Corresponsabilità Educativa all'inizio di ogni ciclo scolastico. Una versione sintetica e adattata all'età del documento viene diffusa all'interno delle attività didattiche di educazione alla cittadinanza.

2. Le Regole per l'Uso delle Tecnologie a Scuola

L'Istituto si impegna a promuovere la cultura della sicurezza online. Per garantire un ambiente sicuro, ci sono regole precise sull'utilizzo di Internet e degli strumenti digitali:

A. Accesso alla Rete e ai Dispositivi Scolastici

- L'accesso a Internet e la navigazione attraverso le strumentazioni scolastiche è riservato a un **uso strettamente didattico**.



Ministero dell'Istruzione e del Merito

Istituto comprensivo statale “ Ernesto Balducci” di Fiesole eVaglia

- È **vietato l'accesso a internet senza l'autorizzazione** da parte del personale docente e in loro assenza.
- La tua attività online all'interno degli spazi scolastici è **monitorata e supportata** per promuovere un uso sicuro e responsabile della rete. L'accesso alla rete è schermato da filtri che impediscono il collegamento a siti non idonei alla didattica.
- **Sei responsabile** del dispositivo che ti viene assegnato. Eventuali violazioni sono sanzionate secondo il Regolamento d'Istituto.

B. Uso degli Account e dei Dati

- Se sei uno studente della scuola secondaria di primo grado, hai un indirizzo e-mail istituzionale (@comprensivofiesole.edu.it) con durata triennale, che ti permette di comunicare e condividere materiali **solo con i membri interni all'Organizzazione**.
- **Non devi salvare** dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche.
- Devi usare le tue credenziali (username e password) in modo responsabile e custodirle con cura.
- È vietato scaricare da internet materiale senza l'autorizzazione del docente.

3. Comportamenti Non Ammessi (Infrazioni)

Il tuo comportamento online è considerato come quello nell'ambiente fisico. Le violazioni dell'ePolicy saranno gestite privilegiando sempre un **approccio educativo e formativo**, ma in presenza di comportamenti gravi, la scuola può prevedere sanzioni disciplinari.

Sono considerate condotte sanzionabili o oggetto di intervento educativo le seguenti azioni:

- **Cyberbullismo:** Utilizzare la rete per giudicare, offendere, denigrare o escludere altri, o per esprimersi in modo volgare o aggressivo.
- **Privacy e Dati:** Condividere in modo incauto o non autorizzato le tue foto, dati personali o informazioni sensibili (es. indirizzo, numero di telefono).
- **Diffusione Immagini:** Pubblicare o diffondere online immagini o video di compagni/e o del personale scolastico **senza consenso**, in particolare se sono offensivi o denigratori.
- **Contenuti Inappropriati:** Condividere o inviare contenuti intimi o a sfondo sessuale (propri o altrui).
- **Esclusione:** Inviare immagini o video finalizzati a escludere o emarginare altri studenti o studentesse.
- **Comunicazioni non autorizzate:** Comunicare online in modo non autorizzato o imprudente con sconosciuti.
- **Navigazione non consentita:** Accedere a siti web non idonei o non indicati dai docenti durante le attività didattiche.

4. Sensibilizzazione e Prevenzione



Ministero dell'Istruzione e del Merito

Istituto comprensivo statale “ Ernesto Balducci” di Fiesole eVaglia

La scuola ti aiuta a sviluppare le competenze digitali per usare le tecnologie con sicurezza, spirito critico e responsabilità.

- Verranno realizzate **lezioni dedicate** alle buone pratiche digitali, ai rischi della rete e alla prevenzione del cyberbullismo.
- La scuola utilizza risorse e programmi come il **Kit Didattico** e i percorsi formativi disponibili sulla piattaforma di *Generazioni Connesse*.
- L'Istituto promuove la riflessione e il rispetto delle regole di convivenza digitale, in quanto le condotte scorrette sono considerate occasioni educative.

5. Segnalazione e Supporto

Se tu, o un tuo compagno/a, state vivendo una situazione problematica (come cyberbullismo, adescamento online o sexting), è fondamentale chiedere aiuto.

Chi puoi avvisare a scuola? Qualunque problematica, violazione o abuso, anche online, deve essere segnalata tempestivamente.

1. **I/le tuoi/tue docenti.**
2. **Il Dirigente Scolastico.**
3. **Il Referente per il Cyberbullismo e Bullismo.**
4. **Il Team di docenti "antibullismo".**

Come puoi segnalare? La scuola si impegna a mettere a tua disposizione strumenti specifici per aiutarti a segnalare, anche in forma anonima:

- Un indirizzo e-mail specifico per le segnalazioni.
- Una scatola/box per la raccolta di segnalazioni anonime (collocata in uno spazio accessibile e ben visibile).
- Uno sportello di ascolto con professionisti.
- Il docente referente per le segnalazioni.

Servizi esterni di supporto: Puoi anche rivolgerti a servizi esterni come la **Helpline 19696** e la Chat di Telefono Azzurro, utili per ricevere supporto e consulenza.

In caso di episodi di particolare gravità, la scuola valuterà la segnalazione alle autorità competenti (come la Polizia Postale) e attiverà supporti psicologici o di mediazione, coinvolgendo i servizi territoriali competenti.

Per ulteriori dettagli e procedure specifiche (inclusa la gestione di eventuali infrazioni), si rimanda al Regolamento d'Istituto, al Patto di Corresponsabilità Educativa e al Codice Interno per il contrasto dei fenomeni di Bullismo e Cyberbullismo, tutti consultabili sul sito web scolastico.



Ministero dell'Istruzione e del Merito

Istituto comprensivo statale “ Ernesto Balducci” di Fiesole e Vaglia

Documento Sintetico Informativo per i Genitori

ePolicy dell'Istituto Comprensivo E. Balducci di Fiesole e Vaglia

Gentili Genitori,

Questo documento sintetico è stato creato per illustrarvi gli obiettivi e i principi fondamentali dell'ePolicy adottata dal nostro Istituto, un documento programmatico e operativo essenziale per la costruzione della cittadinanza digitale all'interno della comunità educante.

1. Scopo e Obiettivi dell'ePolicy

L'ePolicy è un documento di riferimento condiviso che mira a promuovere l'uso delle tecnologie digitali in modo positivo, critico e consapevole da parte degli studenti e delle studentesse, sotto la guida degli adulti coinvolti nel processo educativo. L'obiettivo è garantire il benessere digitale e la sicurezza in Rete.

L'ePolicy lavora su quattro obiettivi principali:

1. Promuovere l'uso sicuro e responsabile della rete nell'intera comunità scolastica.
2. Prevenire e sensibilizzare sui comportamenti online a rischio.
3. Definire norme comportamentali e procedure per l'uso delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico.
4. Stabilire misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate a un uso non corretto delle tecnologie digitali.

2. Il Vostro Ruolo (Genitori/Adulti di Riferimento)

Voi siete considerati attori partecipi e attivi nella promozione e nell'educazione all'uso consapevole delle ICT e della Rete, in continuità con le azioni dell'Istituto.

È fondamentale che:

- Accettiate e condividiate quanto stabilito nell'ePolicy e nel Patto di Corresponsabilità, in un'ottica di reciproca collaborazione.
- Vi impegniate a partecipare in maniera proattiva agli eventi formativi/informativi organizzati dall'Istituto.
- Comuniciate con i docenti in merito a problemi riscontrati quando i vostri figli non usano responsabilmente le tecnologie digitali o Internet.



Ministero dell'Istruzione e del Merito

Istituto comprensivo statale “ Ernesto Balducci” di Fiesole eVaglia

L'ePolicy è stata integrata nel Patto di Corresponsabilità Educativa e nel Regolamento d'Istituto, che vengono aggiornati con riferimenti specifici. All'inizio di ogni ciclo scolastico, l'ePolicy viene presentata ai genitori e agli alunni insieme al Patto di Corresponsabilità.

3. Sensibilizzazione e Prevenzione

La scuola è impegnata a sviluppare azioni e interventi per promuovere una cittadinanza digitale che includa la conoscenza dei diritti, dei rischi e delle opportunità online.

Per raggiungere questo scopo:

- L'Istituto ha predisposto un Curricolo Digitale (basato sul framework europeo DigComp 2.2) per sviluppare le competenze digitali negli insegnamenti disciplinari.
- Vengono realizzate lezioni dedicate alle buone pratiche digitali, ai rischi della rete e alla prevenzione del cyberbullismo.
- La scuola utilizza il Kit Didattico del progetto *Generazioni Connesse* come risorsa metodologica per le attività di Educazione Civica Digitale (ECD) in classe.

4. Gestione dei Dispositivi e Regole di Comportamento

L'ePolicy definisce le norme per l'utilizzo degli strumenti tecnologici (ICT) nella scuola:

- L'accesso ad Internet da parte degli alunni è ammesso solo in presenza del docente ed esclusivamente per motivi didattici. L'accesso è schermato da filtri di sicurezza.
- L'Istituto utilizza piattaforme sicure come il Registro Elettronico e Google Workspace for Education, accessibili tramite credenziali personali fornite dalla scuola.
- L'Istituto considera l'ambiente online alla stregua dell'ambiente fisico, garantendo la sicurezza attraverso misure tecniche (firewall, reti separate tra didattica e segreteria, monitoraggio degli accessi).
- Per la gestione degli strumenti personali (BYOD - *Bring Your Own Device*), si fa riferimento al Patto di Corresponsabilità, ai Regolamenti di Istituto e alle normative ministeriali vigenti.

Cosa costituisce un uso improprio delle tecnologie (esempi di condotte sanzionabili o oggetto di intervento educativo):

- Utilizzo della rete per giudicare, offendere, denigrare o escludere altri, o per esprimersi in modo volgare o aggressivo.
- Condivisione incauta o non autorizzata di dati personali o sensibili.
- Pubblicazione o diffusione online di immagini o video di compagni/e o del personale scolastico senza consenso, in particolare se offensivi o denigratori.
- Accesso a siti web non idonei durante le attività didattiche.

Le violazioni saranno gestite dando sempre la priorità a un approccio educativo e formativo, ma la scuola può prevedere sanzioni disciplinari in caso di comportamenti più gravi, nel rispetto del Regolamento d'Istituto.



Ministero dell'Istruzione e del Merito

Istituto comprensivo statale “ Ernesto Balducci” di Fiesole eVaglia

5. Segnalazione e Gestione dei Casi

L'ePolicy include procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio (come cyberbullismo, sexting o adescamento online).

Chi interviene:

- Il Dirigente Scolastico ha un ruolo centrale e ha il compito di informare tempestivamente e coinvolgere le famiglie in caso di situazioni problematiche, ad eccezione dei casi sospetti che richiedono la segnalazione diretta alle Forze dell'Ordine.
- L'Istituto ha un Team Anti-bullismo e per l'Emergenza (coordinato dal Dirigente Scolastico) e Referenti per il bullismo e cyberbullismo che definiscono gli interventi di prevenzione e gestiscono i casi.
- In caso di episodi di particolare gravità, la scuola valuta la segnalazione alle autorità competenti (ad esempio la Polizia Postale) e può attivare supporti psicologici o di mediazione, coinvolgendo i servizi territoriali.

Come Segnalare:

- Anche i genitori possono e devono segnalare casi di sospetto o evidenza di fenomeni problematici.
- La segnalazione va indirizzata al Dirigente Scolastico, al docente coordinatore di classe, al referente d'istituto o direttamente al team antibullismo (attraverso apposite procedure definite dall'istituto).
- Per supporto e consulenza, i genitori possono rivolgersi alla Helpline del progetto *Generazioni Connesse*, al numero gratuito 19696.

6. Informazioni e Contatti

L'Istituto si impegna a diffondere l'ePolicy attraverso:

- La pubblicazione sul sito istituzionale della scuola (sia in versione integrale che sintetica).
- La consegna della versione sintetica rivolta alle famiglie durante i colloqui scuola-famiglia.

Per ulteriori dettagli e approfondimenti, si rimanda alla sezione “Regolamento d'Istituto” del sito web scolastico, dove sono consultabili tutti i regolamenti dell'Istituto Comprensivo E. Balducci.

Ringraziando per la Vostra collaborazione, essenziale per garantire un uso sicuro e responsabile delle tecnologie per tutti gli studenti.