



## Dokument ePolicy

Fachoberschule für Wirtschaft, Grafik und Kommunikation  
Julius und Gilbert Durst

ePolicy

Diese ePolicy basiert auf

- dem EU-Rahmen für digitale Schlüsselkompetenzen,
- der EU-Strategie „Better Internet for Kids“,
- dem Projekt Safer Internet Centre Italia (EU-kofinanziert),
- den italienischen Bildungs- und Jugendschutzgesetzen sowie
- dem Prinzip der schulischen Autonomie und Partizipation.

Die hier genutzte Vorlage von Generazioni Connesse wurde im Rahmen des **italienischen Safer Internet Centre (SIC)** entwickelt. Das Projekt **Generazioni Connesse** wird

- vom **Ministerium für Bildung und Leistung (MIM)** koordiniert,
- von der **Europäischen Kommission kofinanziert** (Connecting Europe Facility) und
- gemeinsam mit Partnern wie der Post- und Kommunikationspolizei, Universitäten und Kinderschutzorganisationen umgesetzt.

Die ePolicy ist dabei als **Standardtext mit individuell anpassbaren Teilen** konzipiert, der allen italienischen Schulen zur Verfügung steht.

Der Standardtext ist in italienischer Sprache formuliert, die individuell an unsere Schule angepassten Teile sind in deutscher Sprache eingefügt, womit ein bilinguales Dokument vorliegt.

In diesem Dokument wird auf die Verwendung gendergerechter Sonderzeichen (z. B. \*, :, \_) bewusst verzichtet. Die Entscheidung dient der **Wahrung der sprachlichen Klarheit, Lesbarkeit und Einheitlichkeit** des Textes. Die verwendeten Personenbezeichnungen sind **generisch gemeint** und schließen ausdrücklich **alle Geschlechter und Geschlechtsidentitäten** ein.

---

La presente ePolicy si basa su

- il quadro di riferimento dell'UE sulle competenze chiave digitali,
- la strategia dell'UE «Better Internet for Kids»,
- il progetto Safer Internet Centre Italia (cofinanziato dall'UE),
- le leggi italiane in materia di istruzione e tutela dei minori, nonché
- il principio dell'autonomia scolastica e della partecipazione.

Il modello di Generazioni Connesse qui utilizzato è stato sviluppato nell'ambito del Safer Internet Centre (SIC) italiano. Il progetto Generazioni Connesse è

- **coordinato dal Ministero dell'Istruzione e delle Competenze (MIM),**
- **cofinanziato dalla Commissione Europea (Connecting Europe Facility) e**
- **realizzato in collaborazione con partner quali la Polizia delle Poste e delle Comunicazioni, le università e le organizzazioni per la tutela dei minori.**

La ePolicy è concepita come testo standard con parti personalizzabili, a disposizione di tutte le scuole italiane.

Il testo standard è redatto in lingua italiana, mentre le parti adattate alla nostra scuola sono inserite in lingua tedesca, rendendo il documento bilingue.

In questo documento si rinuncia consapevolmente all'uso di caratteri speciali di genere (ad es. \*, :, \_). La decisione serve a garantire la chiarezza linguistica, la leggibilità e l'uniformità del testo. I termini utilizzati per indicare le persone hanno un significato generico e includono espressamente tutti i generi e le identità di genere.

# 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' ePolicy 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.

### Was bedeutet das für unsere Schule?

Die Fachoberschule für Wirtschaft, Grafik und Kommunikation „Julius und Gilbert Durst“ führt diese ePolicy mit dem Ziel ein, das digitale Umfeld in ein Übungsfeld für aktive Bürgerschaft und berufliche Qualifizierung zu verwandeln. Im Einklang mit den Fachrichtungen Wirtschaft, Grafik und Kommunikation setzt sich die Schule folgende konkrete Ziele:

- Förderung einer bewussten und strategischen Nutzung der Technologien von Kollaborationsplattformen (Google Workspace / Microsoft Teams) nicht nur als Speicherorte, sondern als Umgebungen für integrierten und praxisorientierten Unterricht. Ziel ist es, bei den Schülern die digitalen Soft Skills zu entwickeln, die sowohl im Studium als auch auf dem Arbeitsmarkt erforderlich sind, und dabei die Inklusion aller zu gewährleisten.
- Erziehung zu rechtlicher und ethischer Verantwortung im Internet. Im Schwerpunkt Wirtschaft liegt der Fokus auf Datensicherheit und digitaler Finanzwirtschaft; im Schwerpunkt Grafik und Kommunikation konzentriert sich die Prävention auf die Einhaltung des Urheberrechts, die Überprüfung von Quellen (Bekämpfung von Fake News) und den ethischen Umgang mit Bildern, um Cybermobbing und digitaler Manipulation entgegenzuwirken.
- Vertikale Lehrpläne für digitale Staatsbürgerkunde umsetzen, die sich kritisch mit den Themen Online-Identität, Umgang mit personenbezogenen Daten und Respekt gegenüber anderen auseinandersetzen und so aktiv Phänomene wie Isolation oder Übergriffe verhindern.
- Die Bedeutung der „Podcast“- und „Virtual-Reality“-Labore als Räume für sicheres Experimentieren stärken.
- Klare und gemeinsam vereinbarte Regeln für die Nutzung eigener Geräte (BYOD) und schulischer Geräte festlegen, die auf individuelle Verantwortung ausgerichtet sind. Das Ziel ist es, unter Einhaltung der ministeriellen Gesetze und der schulischen Vorschriften, von einem einfachen „Verbot“ zu einer „bewussten und kritischen Entscheidung“ für das Lernen mit geeigneten Werkzeugen zu gelangen.
- Klare Regeln für die Nutzung der Fachlabore und der eigenen Geräte (BYOD) festlegen. Ziel ist es, den Schülern den Unterschied zwischen der spielerischen/privaten Nutzung des Smartphones und der professionellen Nutzung des technologischen Geräts unter Einhaltung der schulischen und institutionellen Netiquette verständlich zu machen.
- Festlegung einfacher und vertrauenswürdiger Verfahren, damit Schüler und Personal Probleme oder den Missbrauch von Technologien melden können. Die Schule gewährleistet in Zusammenarbeit mit den Administratoren der verwendeten Lernplattformen, dem Innovationsteam und dem Beauftragten für Cybermobbing eine sofortige pädagogische Intervention, die nicht nur auf Sanktionen ausgerichtet ist. Der Umgang mit kritischen Situationen wird als Gelegenheit zur angeleiteten Reflexion über die rechtlichen und sozialen Folgen von Handlungen in digitalen Umgebungen verstanden.
- Die Schule nutzt spezielle Lernplattformen: Google Workspace for Education und Microsoft Teams als primäres Umfeld für die Kommunikation, den Austausch von Materialien und die Zusammenarbeit auf Distanz.

Die Nutzung dieser Umgebungen dient ausschließlich didaktischen Zwecken und erfolgt unter der Aufsicht der Lehrkräfte, wodurch die Wahrung der Privatsphäre und der Schutz der personenbezogenen Daten von Minderjährigen gewährleistet werden. In diesem Zusammenhang besteht der Zweck der ePolicy darin, die Zugangsmodalitäten, die Nutzungszeiten und die Verhaltensregeln (Netiquette) festzulegen, die Schüler und Mitarbeiter in den virtuellen Klassenräumen einhalten müssen.

## 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 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 (Tecnologie dell'Informazione e della Comunicazione, o ICT in inglese).

## 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.

## Was bedeutet das für unsere Schule?

Die Fachoberschule für Wirtschaft, Grafik und Kommunikation „Julius und Gilbert Durst“ versteht die Umsetzung der ePolicy als einen gemeinschaftlichen und schrittweisen Prozess. Um das Dokument in die Praxis umzusetzen, werden folgende Rollen und vorrangige Aufgaben festgelegt:

*Der Schulleiter* fördert die Einführung von IT-Sicherheitsprotokollen und stellt sicher, dass die ePolicy in den Schulentwicklungsplan integriert wird. Er stützt sich dabei auf die Unterstützung des Datenschutzbeauftragten, um zu gewährleisten, dass die Nutzung der Lernplattformen und der digitalen Tools den Datenschutzbestimmungen entspricht. Der digitale Koordinator, die Administratoren der Lernplattformen und das Innovationsteam fungieren als „technologische Vermittler“. Ihre Hauptaufgabe ist die technische Verwaltung der institutionellen Konten und die Unterstützung der Kollegen bei der kritischen Nutzung der Tools. Sie gewährleisten, dass die Schüler in einer sicheren und geschützten Umgebung navigieren.

*Der Ansprechpartner für Cybermobbing und das Anti-Mobbing-Team* sind die Anlaufstelle für den Umgang mit kritischen Situationen. Ihre Rolle ist in erster Linie präventiv: Sie sammeln etwaige Meldungen von Lehrkräften oder Schülern und aktivieren, wo nötig, die Protokolle zum Umgang mit Online-Belästigungen in Absprache mit dem betroffenen Klassenrat.

*Die Lehrkräfte* sind die täglichen Vermittler der Regeln. Insbesondere Lehrkräfte der fachrichtungsspezifischen Fächer (Informatik, Wirtschaft, Recht und Grafik) integrieren in ihre Lehrpläne Module zu digitaler Ethik, Urheberrecht und Datensicherheit. Jede Lehrkraft ist für die Aufsicht bei der Nutzung der Geräte im Unterricht oder in den Spezialräumen verantwortlich.

*Die Schülerinnen und Schüler* sowie ihre Vertreter sind dazu aufgerufen, proaktive Nutzer zu sein, d. h. sie müssen lernen, ihre digitale Identität selbstständig zu verwalten, aktiv an der Lösung einfacher technischer Probleme mitzuwirken und sich innerhalb der Klasse für gute Netiquette-Praktiken einzusetzen. Die Schülervertreter nehmen an der jährlichen Überarbeitung der ePolicy teil, indem sie die Bedürfnisse der Schüler vertreten und unter Gleichaltrigen (Peer Education) die Einhaltung der schulischen Netiquette fördern.

*Die Familien* erklären sich mit der Unterzeichnung der ePolicy bereit, die Mediennutzung ihrer Kinder im häuslichen Umfeld verantwortungsvoll zu begleiten und bei auftretenden Risikosituationen die Schule zu informieren.



## 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'ePolicy, 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.

### Was bedeutet das für unsere Schule?

Unsere Schule nimmt die ePolicy in die wichtigsten Schuldokumente (Dreijahresplan, Schulordnung, Schülercharta) auf, um eine gemeinsame digitale Kultur zu fördern. Die Integration erfolgt wie folgt:

Die ePolicy bestätigt die bereits bestehenden Regeln für die Nutzung von Google Workspace Plus. Diese Regeln gelten auch für die Nutzung von Mac- und PC-Computern in den verschiedenen Computerräumen der Schule. Die Schüler müssen diese Geräte sorgfältig nutzen und die Arbeit anderer sowie die Urheberrechtsgesetze respektieren.

BYOD-Projekt (ab den ersten Klassen im Schuljahr 2025/26) - Die ePolicy legt fest, wie persönliche Geräte (Tablets, PCs und Chromebooks), die die Schüler von zu Hause mitbringen, ordnungsgemäß zu nutzen sind. Das Ziel ist es, das eigene Gerät im Unterricht ausschließlich für schulische Zwecke und auf sichere Weise zu nutzen.

Dank der fast zehnjährigen Erfahrung unseres Fachrichtungsschwerpunktes „Digitale Klasse“ verfügt die Schule über bewährte Handlungsmodelle für einen positiven und kritischen Umgang mit dem Internet.

Der Partnerschaftsvertrag fordert die Eltern auf, mit der Schule zusammenzuarbeiten. Gemeinsam helfen wir den Jugendlichen, ihre Schulprofile und ihre Geräte verantwortungsbewusst zu nutzen und Risiken wie Cybermobbing vorzubeugen.

Politische Bildung - Die ePolicy wird zum Leitfaden für den Unterricht in „Digitaler Bürgergesellschaft“. Die Schüler lernen, dass ihr Online-Verhalten korrekt und professionell sein muss.

## 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.

### **Was bedeutet das für unsere Schule?**

Um unsere ePolicy der gesamten Schulgemeinschaft bekannt zu machen, nutzt die Schule folgende Instrumente:

*Informationen für die Familien* - Das Dokument wird auf der Website der Schule veröffentlicht und über die offiziellen Kanäle (z. B. das elektronische Klassenbuch) versendet. Im Laufe des Jahres prüft die Schule die Möglichkeit, Treffen zu organisieren, um den Eltern der ersten Klassen zu erklären, wie die Lernplattformen genutzt werden, und ihnen dabei zu helfen, ihre Kinder bei der sicheren Nutzung des Internets zu unterstützen.

**Schüleraufklärung** - Die Lehrkräfte stellen die ePolicy im Rahmen des Unterrichts zur Gesellschaftlichen Bildung vor. In den ersten Klassen geschieht dies zu Beginn des BYOD-Projekts. In den Klassen der Oberstufe wird der Zusammenhang zwischen den Schulregeln und den künftigen Regeln der Arbeitswelt vertieft.

**Digitaler Lehrplan (DigComp 3.0)** - Die Schule integriert die europäischen digitalen Kompetenzen in den Unterricht. Die Schüler lernen, mit Daten umzugehen, eigene digitale Inhalte zu erstellen und zu teilen sowie ihre Online-Identität zu schützen.

**Externe Kommunikation** - Die Schule teilt die Grundsätze der ePolicy mit interessierten externen Partnern (z. B. Unternehmen, die Schüler während ihres Praktikums aufnehmen). Wenn die Schule bei Projekten mit digitalen Aktivitäten mit externen Experten zusammenarbeitet, müssen diese die in unserem Dokument beschriebenen Sicherheitskriterien und pädagogischen Werte kennen und einhalten.

**Barrierefreiheit** - Das Informationsmaterial ist so gestaltet, dass es für alle klar und verständlich ist. Die Dokumentation kann mithilfe kostenloser und im Internet leicht zugänglicher Tools in die eigene Sprache übersetzt werden.

---

## 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

## Was bedeutet das für unsere Schule?

Die Schule setzt ihre dreijährigen Ziele um, wobei sie sich auf die langjährige Erfahrung der „Digitalen Klasse“ und die Einführung von BYOD stützt. Die wichtigsten Maßnahmen sind:

### 1. JAHR

Organisation von Treffen, um den Lehrkräften die ePolicy zu erläutern und das Dokument den neuen Familien vorzustellen, wobei die Bedeutung der Sicherheit im Unterricht sowie in den Computer- und Grafikräumen hervorgehoben wird.

Die Nutzungsregeln für Google Workspace Plus und die BYOD-Richtlinien aktualisieren und sicherstellen, dass sie auch für die Schülerinnen und Schüler einfach und verständlich sind.

Den Fortbildungsbedarf der Lehrkräfte analysieren, insbesondere im Hinblick auf den Umgang mit privaten Geräten im Unterricht und den Datenschutz.

## 2. JAHR

Spezifische Kurse für Lehrkräfte zur Nutzung von Unterrichtstools und zum Umgang mit Online-Risiken durchführen, an denen mindestens 60 % des Personals teilnehmen.

Schulungsmaßnahmen für Schüler und Schülerinnen zum Thema „Digitale Bürgerschaft“ unter Verwendung ausgewählter, geprüfter und geeigneter Materialien einleiten.

Die Unterrichtsmaterialien nutzen, um die Nutzung von Tablets und Computern von einem einfachen technologischen Werkzeug zu einer entscheidenden Ressource für das Lernen zu machen.

## 3. JAHR

Die Wirkung der durchgeführten Maßnahmen anhand von Fragebögen für Schülerinnen und Schüler sowie deren Eltern überprüfen. Die Ergebnisse werden dazu beitragen, den Dreijahresplan für das Bildungsangebot zu verbessern.

Schülerinnen und Schüler der vierten oder fünften Klassen als Mentoren für ihre jüngeren Mitschüler einbinden und so einen verantwortungsvollen und professionellen Umgang mit Technologien und Fachräumen fördern.

---

# 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](#)

## Was bedeutet das für unsere Schule?

Zusätzlich zu den Materialien, die vom nationalen Portal „Generazioni Connesse“ in italienischer Sprache bereitgestellt werden, nutzt und fördert unsere Schule die Verwendung geprüfter Plattformen und Ressourcen in deutscher Sprache, um der gesamten Schulgemeinschaft einen möglichst breiten Zugang zu gewährleisten:

- [Saferinternet.at](https://saferinternet.at) - deutschsprachige Ressource, die Lehrmaterialien, Webinare und aktuelle Leitfäden zu den Themen soziale Medien, Datenschutz und neue Technologien bietet.
- [So geht Medien](https://sogehtmedien.de) - deutschsprachige Ressource, die Lehrmaterialien, Webinare und aktuelle Leitfäden zu den Themen soziale Medien, Datenschutz und neue Technologien bietet.
- [Klicksafe.de](https://klicksafe.de) - europäische Initiative, die Informationsmaterialien zum Thema Online-Sicherheit bereitstellt, mit besonderem Schwerpunkt auf Themen wie dem digitalen Urheberrecht und dem kritischen Umgang mit Medien (DigComp).
- [IQES ONLINE](https://iqesonline.it) - deutschsprachige Ressource, die Lehrmaterialien, Webinare und aktuelle Leitfäden zu den Themen soziale Medien, Datenschutz und neue Technologien bietet.
- **Informativa Locale (Provincia Autonoma di Bolzano):** Einbindung von Materialien, die von der Schulbehörde in deutscher Sprache sowie von den Sozial- und Jugendämtern der Region zur Bekämpfung von Cybermobbing erstellt wurden.
- [Google for Education Safety Center](https://googleforeducation.safetycenter.org): Spezifische Ressourcen für die sichere Nutzung von Google Workspace Plus-Konten, mit Anleitungen in mehreren Sprachen.
- **Generazioni Connesse (Safer Internet Centre Italia)** - Nationale Anlaufstelle für Unterrichtsmaterialien, Leitfäden und Meldungsverfahren.
- <https://apa.at/checkbar/checkbar/>: deutschsprachige Ressource, die Lehrmaterialien, Webinare und aktuelle Leitfäden zu den Themen soziale Medien, Datenschutz und neue Technologien bietet.
- <https://bildung.orf.at/>: deutschsprachige Ressource, die Lehrmaterialien, Webinare und aktuelle Leitfäden zu den Themen soziale Medien, Datenschutz und neue Technologien bietet.
- <https://www.medien-in-die-schule.de/>: deutschsprachige Ressource, die Lehrmaterialien, Webinare und aktuelle Leitfäden zu den Themen soziale Medien, Datenschutz und neue Technologien bietet.

## 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.

#### Was bedeutet das für unsere Schule?

Unsere Schule fördert die digitale Sicherheit durch praktische und alltägliche Maßnahmen. Die Hauptziele sind:

##### 1. Für die Schüler: wissen, um vorzubeugen

- Im Lehrplan für Gesellschaftliche Bildung jeder Klasse kurze Module (z. B. 2-3 Stunden pro Jahr) zu spezifischen Themen aufnehmen: In den ersten Klassen liegt der Schwerpunkt auf BYOD und Selbstständigkeit; in den drei Jahren des Grafik- und Wirtschaftszweigs werden spezifische Themen wie Urheberrecht und die Sicherheit beruflicher Daten behandelt.
- Während der Laborstunden schulen die Lehrkräfte die Schüler im richtigen Umgang mit Bildern und im Schutz gemeinsamer Dateien.
- Erfahrenere Schüler helfen jüngeren Mitschülern bei der Konfiguration der Geräte und der Einhaltung der *Netiquette*.

##### 2. Für Lehrkräfte: Fortbildung und Zusammenarbeit

- Organisation kurzer Fortbildungen (auch online) zum sicheren und effektiven Umgang mit Google Workspace Plus (einschließlich fortgeschrittener Funktionen wie KI)
- Erstellen eines gemeinsamen Ordners auf Drive oder eines Kurses in Classroom, in dem Lehrkräfte fertige Materialien finden, um im Unterricht über Cybermobbing oder Datenschutz zu sprechen.

### 3. Für die Familien: Bildungsvereinbarung

- Den Familien einen einfachen Leitfaden mit Regeln für die Computernutzung zu Hause und in der Schule (BYOD-Projekt) zur Verfügung stellen.
- Mindestens einmal im Jahr ein Treffen (auch online) organisieren, das sich mit dem Umgang mit Online-Risiken und den Möglichkeiten schulischer Plattformen befasst.

### 4. Allgemeine Präventionsmaßnahmen

- Allen Schülern vermitteln, an welche Lehrkräfte sie sich bei Problemen oder unangenehmen Erfahrungen im Internet wenden können.
- Schüler und Familien über die App BattBull informieren, die auf das Handy heruntergeladen und - auch anonym - genutzt werden kann, um Fälle von Mobbing und Cybermobbing in der Schule und in der Freizeit zu melden.

---

## 2.2 - Il Curricolo Digitale

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

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

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

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

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

### Was bedeutet das für unsere Schule?

Um die Ziele der digitalen Bürgerschaft zu erreichen, nutzt das Institut nationale und internationale Ressourcen und ordnet die Kompetenzen in den europäischen Rahmenwerken DigComp 2.2 und DigCompEdu ein. Die Aktivitäten sind im Lehrplan für die Erziehung zur digitalen Bürgerschaft (Gesetz 92/2019) verankert und stehen in engem Zusammenhang mit der vorliegenden ePolicy.

Ziel ist es, durch folgende konkrete Maßnahmen mündige digitale Bürger heranzubilden:

- Erste Klassen und BYOD-Projekt: Es ist ein spezieller Lehrplan vorgesehen, um die Schüler im richtigen Umgang mit ihren eigenen Geräten und im verantwortungsvollen Umgang mit ihren Google Workspace-Konten anzuleiten.
- Zweites Biennium sowie fünftes Jahr: Die Schule wendet einen vertikalen Lehrplan nach dem Iprase-Modell an. Die Klassenräte wählen die Themenbereiche und Kompetenzen aus, die für jedes Fach des jeweiligen Bildungszweigs am besten geeignet sind.



- Sprachliche Anpassung: Die Lehrkräfte behalten sich das Recht vor, bei Bedarf den berechtigten Schülern die notwendigen Hilfsmittel zur Verfügung zu stellen, damit diese die Ressourcen effektiv nutzen können, und gewährleisten so einen gleichberechtigten Zugang zur digitalen Bildung.
- Gesellschaftliche Bildung: Jede Klasse widmet spezifische Unterrichtseinheiten der Erörterung der Inhalte der ePolicy und nutzt dabei auf das Alter der Schüler abgestimmte Unterrichtsmaterialien, um ein kritisches Bewusstsein für die Risiken und Chancen des Internets zu fördern.
- Sicherheit in den Computerräumen: Die Prävention umfasst spezifische Unterweisungen zur Nutzung der verschiedenen digitalen Geräte und Dienste, damit die Schüler lernen, das Urheberrecht zu respektieren und ihre professionelle digitale Identität zu schützen.

---

## 2.3 - Il Kit Didattico

L'ePolicy 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'ePolicy 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.

### Was bedeutet das für unsere Schule?

Eine spezielle Arbeitsgruppe wählt die didaktischen Aktivitäten aus dem „Kit Didattico“ von „Generazioni Connesse“ aus. Diese Ressourcen werden Kollegen und Schülern zur Verfügung gestellt und dabei an die verschiedenen Lernstufen sowie an die Anforderungen des zweisprachigen Umfelds angepasst.

Lernpfad für die ersten Klassen: Für das erste Jahr jedes Fachbereichs gibt es bereits einen vollständigen Kurs, der auf dem Rahmenwerk DigComp 2.2 basiert. Der Lehrplan umfasst interaktive Aktivitäten, die darauf abzielen, die Schüler für die Nutzung von BYOD und Google Workspace zu sensibilisieren.

Unterstützung für Lehrkräfte über Classroom: Die Schule hat einen Kurs auf Classroom eingerichtet, der dem gesamten Lehrerkollegium zugänglich ist. Diese Plattform ermöglicht es den Lehrkräften, auf vorgefertigte Materialien zurückzugreifen und diese an die spezifischen Bedürfnisse der Klasse oder des behandelten Fachs anzupassen.

Fachlehrplan und Kompetenzen: Die Lehrpläne der einzelnen Fächer integrieren Methoden und Aktivitäten, die sich auf die Rahmenwerke DigComp 2.2 und DigCompEdu beziehen. Ziel ist es, dass jedes Fach dazu beiträgt, ein kritisches Bewusstsein für die Risiken des Internets und einen professionellen Umgang mit Technologien zu entwickeln.

[Fachcurricula](https://fo-brixen.it/infos-schueler-innen/fachcurricula-und-rahmenrichtlinien/) - <https://fo-brixen.it/infos-schueler-innen/fachcurricula-und-rahmenrichtlinien/>

# 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.

### Was bedeutet das für unsere Schule?

**Urheberrecht und Softwarelizenzen:** Die gesamte auf den Schulcomputern installierte Software (einschließlich der Grafik- und Wirtschaftsprogramme) ist urheberrechtlich geschützt und an die Schule lizenziert. Das Kopieren, Installieren oder Herunterladen von Programmen ohne Genehmigung ist strengstens untersagt. Wer Raubkopien installiert oder gegen die Lizenzbedingungen verstößt, begeht eine Straftat und kann zivil- und strafrechtlich verfolgt werden.

**Dateiverwaltung und geistiges Eigentum** Die von den Schülern während des Unterrichts erstellten Daten können in den dafür vorgesehenen Bereichen (Google Workspace oder lokale Server) gespeichert werden. Es ist nicht gestattet, die Arbeiten anderer Schüler oder Lehrkräfte ohne Erlaubnis zu verändern, zu löschen oder weiterzugeben. Dies ist besonders wichtig in den Grafik-Labors, wo die Achtung des geistigen Eigentums Teil der beruflichen Ausbildung ist.

### Datensicherung und -speicherung

- **Jährliche Bereinigung:** Am Ende jedes Schuljahres können die lokal auf den Arbeitsplätzen gespeicherten Daten aus Wartungsgründen gelöscht werden.
- **Verantwortung:** Die Nutzer (Schüler und Lehrkräfte) sind für die Sicherung ihrer eigenen Dateien verantwortlich (mithilfe von Google Drive oder externen Speichermedien). Die Schule haftet nicht für Datenverluste aufgrund technischer Störungen.
- **IT-Support:** Das technische Personal darf ausschließlich zu Support- und Systemsicherheitszwecken auf die Daten an den Arbeitsplätzen und im Netzwerk zugreifen.

- Anmeldezeiten und Sicherheit: Der Benutzername und das Passwort sind persönlich und dürfen niemals weitergegeben werden. Jeder Benutzer ist für die Handlungen verantwortlich, die über sein Konto (Workspace oder Mac-Login) vorgenommen werden.
- Umgang mit Bildmaterial und Datenschutz (DSGVO): Gemäß der EU-Verordnung 2016/679 (DSGVO) benötigt die Schule die schriftliche Einwilligung der Eltern (oder volljähriger Schüler) für die Aufnahme und Veröffentlichung von Fotos oder Videos im Zusammenhang mit schulischen Aktivitäten. Es dürfen keine sensiblen Daten auf öffentlich zugänglichen Speichermedien gespeichert werden.
- Verstöße: Die wissentliche Verletzung dieser Vorschriften wird gemäß der Schulordnung geahndet und kann zu einer vorübergehenden Sperrung der Nutzung der Computerräume und des Netzwerks führen.

<https://fo-brixen.it/verwaltung/datenschutz/> - Website der Schule

---

## 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.

### Was bedeutet das für unsere Schule?

#### Allgemeine Nutzung

Die IT-Ausstattung für den Unterricht, mit oder ohne Anbindung an das Intranet des Schulamtes (Unterrichtsdatenleitung), steht allen Schülern und Lehrkräften für den Einsatz im Unterricht und zur Unterrichtsvorbereitung zur Verfügung. Im Einklang mit dem kompetenzorientierten Unterricht werden diese digitalen Medien als Lern- und Arbeitsmittel sowie als Instrumente zur Erfassung, Aufbereitung und Gestaltung von Informationen genutzt. Diese Medien sind insbesondere im Zusammenhang mit dem Internet und dessen Möglichkeiten von Bedeutung. Alle Nutzer der IT-Ausstattung sind verpflichtet, diese Medien angemessen und verantwortungsbewusst zu nutzen. Die Schule und/oder das Aufsichtspersonal ergreifen geeignete Maßnahmen, um eine angemessene und sinnvolle Nutzung der digitalen Medien sicherzustellen. Die Nutzung kostspieliger Geräte (Drucker usw.) muss zudem wirtschaftlichen Erwägungen Rechnung tragen.

#### Wartung

Die Wartung des Systems liegt in der Verantwortung der zuständigen Technikerin (Helene Waldböth) oder der vom Schulleiter ernannten pädagogischen Systemadministratoren (Erwin Mair - Digitales Klassenbuch, Stefan Bergmeister - MS-Teams, Cristina Corbetta - Google Workspace). Neben ihrer Rolle als Berater für den didaktischen und methodischen Einsatz von Medien gewährleisten sie im Rahmen ihres Auftrags den bestmöglichen Betrieb des Systems; nur sie sind befugt, Änderungen an der Konfiguration, den Systemeinstellungen und den Programminstallation vorzunehmen. Sie treffen die erforderlichen Vorkehrungen in Übereinstimmung mit den geltenden Vorschriften zum Datenschutz und zur Datensicherheit.

Störungen an Geräten oder am System sind unverzüglich dem IT-Systemadministrator zu melden. Der Administrator leitet die erforderlichen Maßnahmen gemäß der Richtlinie Nr. 2/2010 (Konzept zur IT-Wartung im Bildungsbereich) ein. Jedes Verhalten, das die Sicherheit und Funktionsfähigkeit der IT-Geräte gefährdet, ist untersagt: Essen, Trinken, Rennen, Werfen von Gegenständen, Umgang mit Flüssigkeiten und scharfen Gegenständen usw. Vor dem Verlassen des Arbeitsplatzes müssen sich die Benutzer ordnungsgemäß vom System abmelden und den Arbeitsplatz sauber und ordentlich hinterlassen. Die Geräte sind gemäß den mit der Schule getroffenen Vereinbarungen auszuschalten. Mobile IT-Geräte sind ordnungsgemäß aufzubewahren oder nach der Nutzung zurückzugeben. Personen, die vorsätzlich oder fahrlässig Schäden verursachen, einschließlich Systemschäden durch Veränderung oder Manipulation der Software, werden zur Verantwortung gezogen.

### **Nutzung von Online-Diensten**

Das Internet ermöglicht den Zugriff auf Informationen und die Kommunikation mit anderen Nutzern weltweit. Die Schule kommt ihrer Aufsichtspflicht und ihrem Schutzauftrag gegenüber Minderjährigen durch regelmäßige und stichprobenartige Kontrollen des Datenverkehrs und der Online-Aktivitäten im schulischen Netzwerk nach. Sie ist zudem berechtigt, den Datenverkehr in Protokolldateien zu speichern, aus denen Nutzer, Daten und Nutzungsarten hervorgehen. Sie kann zudem sogenannte Filtersoftware einsetzen, die jedoch keine vollständige Sperrung fragwürdiger Websites ermöglicht. Im schulischen Rahmen ist der Zugriff auf Websites untersagt, die religiöse, moralische, ideologische oder ethische Empfindlichkeiten verletzen könnten oder die rassistische/faschistische Äußerungen enthalten oder zu Gewalt und Straftaten aufrufen.

Es ist verboten, die Internetverbindung der Schule zu nutzen, um Informationen zu verbreiten, die dem Ruf der Schule schaden könnten. Es ist nicht gestattet, im Namen der Schule vertragliche Vereinbarungen zu treffen oder kostenpflichtige Internetdienste über das Schulnetzwerk zu nutzen.

Bei der Online-Kommunikation über das Schulnetzwerk müssen die Nutzer eine angemessene Sprache verwenden und die Regeln der Netiquette einhalten. Das bedeutet, dass keine beleidigenden, anstößigen oder moralisch bzw. ethisch fragwürdigen Ausdrücke oder Formulierungen verwendet werden dürfen.

### **Google Workspace und Labore**

Das Institut übernimmt als PUA die „*Nutzungsbedingungen von Google Workspace*“, ergänzt durch spezifische Richtlinien für die Nutzung der *Mac-, VR/AR-, Informatik- und Podcast-Labore sowie des BYOD-Projekts*. Das aktualisierte Dokument enthält Verfahren zur Meldung unangemessener Inhalte sowie zweisprachige Netiquette-Regeln für Schüler und Lehrkräfte.

[https://fo-brixen.it/wp-content/uploads/2024/08/2024\\_Informationen-und-Nutzungsbedingungen-der-Google-G-Suite-for-Education-1-1.pdf](https://fo-brixen.it/wp-content/uploads/2024/08/2024_Informationen-und-Nutzungsbedingungen-der-Google-G-Suite-for-Education-1-1.pdf)

Anhang zu den Nutzungsbedingungen von Google Workspace:

#### **1. Nutzung der Fachlabore**

- Professionelle Zwecke - Die Nutzung der Arbeitsplätze und Geräte ist ausschließlich für Lehrzwecke vorbehalten.
- Hardware-Integrität - Es ist verboten, Kabel zu manipulieren, Systemeinstellungen zu ändern oder Software/Schriftarten ohne die Genehmigung des Dozenten oder des technischen Assistenten zu installieren.
- Geistiges Eigentum - Druckgeräte müssen unter Einhaltung des Urheberrechts genutzt werden; das Drucken von urheberrechtlich geschütztem Material ohne Lizenz oder ohne nachgewiesenen didaktischen Zweck ist nicht gestattet.
- Wartung: Jede Störung muss unverzüglich der unterrichtenden Lehrkraft oder dem anwesenden technischen Assistenten gemeldet werden.

## 2. Richtlinien für das BYOD-Projekt

- **Sichere Verbindung:** Schüler, die am BYOD-Projekt teilnehmen, dürfen ihre Geräte nur mit dem dafür vorgesehenen WLAN-Netzwerk verbinden und dabei die von der Schule bereitgestellten Zugangsdaten verwenden.
- **Verantwortung für das Gerät:** Der Schüler ist allein verantwortlich für die Aufbewahrung und den ordnungsgemäßen Betrieb seines persönlichen Geräts.
- **Nutzung im Unterricht:** Das Gerät darf nur auf Aufforderung des Lehrers und für Zwecke genutzt werden, die in direktem Zusammenhang mit dem Unterricht stehen.
- **Datenschutz und Aufzeichnungen:** Es ist strengstens untersagt, das eigene Gerät ohne ausdrückliche pädagogische Genehmigung zur Aufnahme von Audio- oder Videomaterial oder zum Fotografieren von Mitschülern oder Schulpersonal zu verwenden.

## 3. Sicherheits- und Meldeverfahren

- **Unbeabsichtigtes Aufrufen:** Sollte versehentlich eine Website mit unangemessenen Inhalten (gewalttätig, unangebracht oder rechtswidrig) geöffnet werden, darf der Schüler das Fenster nicht schließen oder den Computer ausschalten, sondern muss unverzüglich die Lehrkraft zur Überprüfung benachrichtigen.
- **Zweisprachige Netiquette:** Jede digitale Kommunikation (E-Mails, Kommentare in Classroom) muss den Regeln der Höflichkeit entsprechen: nicht schreien (Großbuchstaben vermeiden), die Meinungen anderer respektieren und eine professionelle Sprache verwenden.

---

## 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.

### Ziele von BYOD im Unterricht:

Die Nutzung des Internets und von Laptops oder die Verwendung digitaler Ressourcen ersetzt in keiner Weise Papier, Stift, Bücher, handwerkliches Arbeiten, reale/direkte Kommunikation und orts- und zeitgebundene Zusammenarbeit, sondern stellt vielmehr eine bereichernde Ergänzung dar, die folgende Ziele verfolgt:

- Es wird ein kooperativer, selbstständiger und selbstorganisierter Lernprozess gefördert.
- Der Unterricht mit den neuen Medien ist motivierend und interaktiv (Erleben, Experimentieren, Entdecken).

- Die Informationen werden aus verschiedenen Medien und Quellen bezogen, ausgewertet und effizient genutzt (Recherche, Präsentation, Modellierung, Simulation).
- Die Arbeit mit Lernplattformen unterstützt die Nutzung und den Austausch gemeinsamer Daten und erleichtert so organisatorische Prozesse (unabhängig von Ort und Zeit).
- Realistische, aktuelle und offene Arbeitsmethoden fördern vernetztes Denken und Problemlösungsfähigkeiten.
- Bestimmte operative Tätigkeiten (Entwurfs-, Strukturierungs- und Berechnungstechniken) werden vom Gerät ausgeführt, wodurch der Arbeitsprozess vereinfacht wird und Arbeiten und Lernen auf verschiedenen Anwendungsebenen ermöglicht werden.
- Die technische Unterstützung ermöglicht und erleichtert die Individualisierung des Lern- und Arbeitsprozesses.
- Der Unterricht entwickelt und stärkt digitale Kompetenzen und ermöglicht es den Lernenden, neue Wege des Wissenserwerbs und Instrumente für lebenslanges Lernen zu entdecken.
- Der lehrergeführte Umgang mit digitalen Medien ermöglicht es den Schülern, den verantwortungsvollen Umgang mit Informationen in der digitalen Welt zu erlernen und ihr Bewusstsein für achtsames Verhalten im digitalen Raum zu schärfen.

### Technische, organisatorische und didaktische Grundsätze

Jeder Schüler bringt sein eigenes digitales Gerät (Tablet, Laptop) mit in den Unterricht - BYOD.

- Das Gerät gilt als Teil des Unterrichtsmaterials, das mit in den Unterricht gebracht wird (ähnlich wie Papier, Stifte und Arbeitshefte).
- Die Schüler sorgen dafür, dass ihr Gerät sofort einsatzbereit ist (aufgeladen und funktionsfähig).

Die Lehrkräfte unterstützen den effektiven Einsatz des Geräts.

- Das Gerät wird regelmäßig im Unterricht eingesetzt, insbesondere wenn es einen pädagogischen Mehrwert bietet.
- Die Lehrkräfte initiieren Lernprozesse im Bereich Medienkompetenz und digitale Kompetenzen im Rahmen ihres Unterrichts (siehe Lehrpläne der einzelnen Fächer).
- Die Schüler werden bei der Nutzung des Geräts von ihren Klassensprechern unterstützt. IT-Administratoren leisten bei Bedarf zusätzliche Unterstützung.

Die Schule stellt eine angemessene Infrastruktur zur Verfügung.

- Die Schule bietet kostenlosen WLAN-Zugang.
- Das Gerät kann bei Nichtgebrauch in abschließbaren Schränken aufbewahrt werden.
- Die Schule stellt Ladestationen für die Geräte zur Verfügung.

## 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/lle 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.

## **Was bedeutet das für unsere Schule?**

### **Standardisierte Verfahren zur Meldung und Bearbeitung von Problemen im Zusammenhang mit riskantem Online-Verhalten von Schülerinnen und Schülern**

Um den Phänomenen Mobbing, Cybermobbing, Online-Grooming und Sexting entgegenzuwirken, wird unsere Schule auf zwei Ebenen tätig:

1. Prävention,
2. Umsetzung von operativen Strategien und Fallmanagement.

#### **PRÄVENTION**

Um die genannten Phänomene zu bekämpfen, darf man sich nicht auf einzelne, einmalige Maßnahmen beschränken, die aus Momenten der Alarmstimmung, der Emotionalität und der Angst heraus erfolgen. Vielmehr ist es notwendig, mit allen verfügbaren Ressourcen zu planen und zu arbeiten, damit die Initiativen für und mit Jugendlichen stetig zunehmen. Prävention zu betreiben, bedeutet daher, in Jugendliche als Bürger zu investieren.

Daher ist ein integrierter Ansatz wichtig, der die Organisation und das Handeln innerhalb der Schule leitet und eine Reihe vereinbarter Ziele festlegt, die den Schülern, dem Personal und den Eltern eine Orientierung und einen greifbaren Beweis für das Engagement unserer Schule zur Prävention und Bekämpfung von Risikoverhalten bieten.

Es sei hier darauf hingewiesen, dass die Präventionsmaßnahmen gegen die genannten Phänomene alle Akteure betreffen, die innerhalb der Schule tätig sind:

#### **Schulleitung:**

1. Benennung eines entsprechend geschulten Lehrers als Ansprechpartner für Initiativen gegen Mobbing, Cybermobbing usw.
2. Einbeziehung der Beratungsstelle (ZIB), wo diejenigen, die das Bedürfnis nach Unterstützung durch Erwachsene haben, eine kommunikative Beziehung zu Psychologen aufbauen können, deren grundlegendes Prinzip das vorurteilsfreie Zuhören ist.

#### **Ansprechpartner für Mobbing/Cybermobbing**

1. Koordiniert Maßnahmen zur Prävention und Bekämpfung dieser Phänomene, unter anderem durch die Zusammenarbeit mit der Postpolizei, den Polizeikräften und den Jugendverbänden vor Ort.
2. Einbindung der Familien in die von der Schule initiierten Präventionsprogramme durch Informationsveranstaltungen.

#### **Lehrerkollegium (vertreten durch einige Lehrkräfte)**

1. Einrichtung eines speziellen Bereichs auf der Startseite der Website der Schule, der der Sammlung nützlicher Materialien zum Thema Mobbing, Cybermobbing usw. sowie der Verbreitung der von der Schule ergriffenen Initiativen dient.
2. Einrichtung einer Datenbank in der Bibliothek (Bücher, Zeitschriften, Filmografie, Websites) zum Thema Mobbing, Cybermobbing usw. sowie zu möglichen Interventionsstrategien
3. Organisation von Fortbildungsmaßnahmen für Lehrkräfte.
4. Organisation von Treffen mit den Schülern, auch unter Einbeziehung von Erfahrungsberichtern und Vorführung von Filmen.
5. Erstellung von Fragebögen zur Beobachtung des Phänomens.
6. Festlegung einfacher Verhaltensregeln gegen Mobbing, Cybermobbing usw., die von allen einzuhalten sind.



## **Klassenrat**

1. Förderung der Aufklärung über den bewussten Umgang mit dem Internet sowie über die Rechte und Pflichten im Zusammenhang mit der Nutzung von Informationstechnologien als Querschnittselement in den verschiedenen Lehrplanfächern.
2. Systematische Beobachtung von Risikoverhalten sowohl bei potenziellen Tätern als auch bei potenziellen Opfern.
3. Scharfe Verurteilung jeder Form von Übergriffigkeit und Intoleranz.
4. Stärkung der emotionalen, sozialen und zwischenmenschlichen Kompetenzen durch Lehrplaninhalte und sozial-emotionale Bildung mittels spezifischer Maßnahmen auf der Grundlage von Peer- und Dispeer-Education.
5. Nutzung kultureller Impulse (Literatur, Filme, Lesungen, Theateraufführungen).
6. Teilnahme an den von der Schule angebotenen außerschulischen Aktivitäten (Projekte).
7. Persönlichkeitsentwicklung der Jugendlichen durch Projekte, die auf Rechts- und Staatsbürgerkunde, Umwelterziehung, Ernährungserziehung und Gesundheitserziehung basieren.

## **Nichtunterrichtendes Personal und Lehrkräfte**

1. Ständige Wachsamkeit seitens des gesamten Schulpersonals.
2. Gewohnheiten und Verhaltensweisen, die Mobbing vorbeugen.

## **DER UMGANG MIT MOBBINGFÄLLEN**

Bei Vorfällen, die diese Phänomene betreffen, ist es wichtig, dass der Schulleiter und der Schulbeauftragte Unterlagen über die Geschehnisse erstellen, darunter Angaben dazu, wer beteiligt war, wo sich die Vorfälle ereignet haben, unter welchen Umständen, wie oft usw., um über objektive Daten zu verfügen. Zu diesem Zweck können verschiedene Methoden angewendet werden, wie z. B.: direkte Beobachtungen und deren Aufzeichnung, Fragebögen für die Schüler, Diskussionen in der Klasse, Gespräche mit einzelnen Schülern.

Sobald die Situation eindeutig geklärt ist, ist folgender Ablauf vorgesehen:

### **Maßnahmen der Lehrkraft**

1. Wenn ein Schüler angibt, Opfer von Mobbing, Cybermobbing usw. zu sein, kontaktiert die Lehrkraft den Schulsozialpädagogen, um einen Termin zu vereinbaren, zu dem sie den Schüler begleitet.
2. Wenn ein Elternteil einen Fall von Mobbing, Cybermobbing usw. gegen sein Kind meldet, erklärt die Lehrkraft, dass die Informationen von der Schulsozialpädagogin erfasst werden, die zu einem Gespräch einladen wird; die Lehrkraft gibt die Kontaktdaten des Elternteils an die Schulsozialpädagogin weiter.
3. Sie informiert die Schulleitung.

### **Maßnahmen der Schulsozialpädagogin (nacheinander)**

1. Gespräch mit dem Opfer zur Klärung der Situation
2. Maßnahmen zur Stärkung des Opfers
3. Gespräch mit dem Täter (auch als mögliche Alternative zur Schulverweigerung)
4. Gegebenenfalls ein Mediationsgespräch zwischen Opfer und Täter
5. Gegebenenfalls ein Treffen mit der gesamten Klasse (Unterstützungsmaßnahmen in der Klasse)
6. Aufbau eines Netzwerks zur Unterstützung, Kommunikation und Zusammenarbeit mit der Familie; Einleitung von Erziehungsmaßnahmen;
7. Berichterstattung über das Ergebnis an die Schulleitung und die Ansprechpartnerin für Mobbing

### **Maßnahmen der Referentin für Mobbing**

1. Sie fungiert als Vermittlerin zwischen Klassenrat, Schulsozialarbeiterin und Schulleitung.
2. Sie notiert und dokumentiert gemeldete Fälle.
3. Sie koordiniert Maßnahmen zur Bekämpfung und Prävention von Mobbing.

### **Maßnahmen der Schulleitung**

1. Wendet sich an den Klassenlehrer, um sich die Situation schildern zu lassen und um eine Beobachtung zu beantragen.
2. Meldet den möglichen Fall der Referentin für Mobbing.
3. Ladet die Eltern der betroffenen Kinder zu einem Gespräch ein (bei Konflikten in Anwesenheit der Schulsozialpädagogin).

4. Fördert in Zusammenarbeit mit den anderen Akteuren Maßnahmen zum Schutz, zur Unterstützung, zur Bekämpfung und zur Resozialisierung.
5. Informiert, falls erforderlich, die zuständigen Behörden.

#### **Maßnahmen des Klassenrates**

1. Eintragung einer sachlichen Beschreibung des betreffenden Verhaltens in das Klassenregister
2. Pünktliche und konsequente Verhängung der in der Schulordnung vorgesehenen Sanktionen
3. Zusammenarbeit mit öffentlichen und/oder privaten Einrichtungen, die den Rehabilitationsprozess der betroffenen Minderjährigen begleiten
4. Im Sinne der Inklusion: Umsetzung eines Projekts, das Folgendes vorsieht: Erfassung des Phänomens durch spezifische quantitative (Fragebogen) und/oder qualitative (Fokusgruppen) Instrumente
5. Persönliche Gespräche mit den Schülern, um Einstellungen wie Angst, resignierte Akzeptanz usw. aufzudecken; Sensibilisierung der Schüler durch verstärkte Information und Aufklärung über das Phänomen; Sensibilisierung der Schüler durch die Förderung von Tugenden wie Mut im Gegensatz zu Schweigen, die Fähigkeit, nach Gewissen und eigenverantwortlich zu entscheiden, Solidarität und das Gefühl, Schwächere zu schützen; Stärkung der sozialen Kompetenzen und Förderung der Zusammenarbeit durch spezifische Interventionsprogramme; Unterstützungsmaßnahmen für Lehrkräfte und Eltern; Überwachung und abschließende Bewertung des Interventionsprojekts
6. Entschiedene Verurteilung jeder Form von Übergriffigkeit und Intoleranz

Es wird darauf hingewiesen, dass die verhängte Sanktion nicht auf den Ausschluss des Schülers aus der Schule abzielen darf, sondern stets darauf ausgerichtet sein muss, den Lernenden innerhalb der Gemeinschaft, der er angehört, zur Verantwortung zu ziehen. Auf der Grundlage der in der Satzung verankerten Grundsätze, die durch die Schulordnung in die autonome Schulrealität umgesetzt werden, muss darauf hingearbeitet werden, dass derjenige, der seine Pflichten verletzt hat, sich nicht nur der sozialen Verwerflichkeit seines rechtswidrigen Verhaltens bewusst wird, sondern auch Maßnahmen ergreift, um den verursachten Schaden wiedergutzumachen.“ (Ministerialdekret vom 05.02.2007, Nr. 16, Allgemeine Leitlinien und Maßnahmen auf nationaler Ebene zur Prävention und Bekämpfung von Mobbing).

#### [Protokoll zur Prävention und Bekämpfung von Mobbing und Cybermobbing](#)

## **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 minorenne.

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

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

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

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

Anche i genitori devono e possono segnalare casi di sospetto o evidenza dei fenomeni, segnalarlo al Dirigente, o al docente

coordinatore di classe o referente di istituto oppure direttamente al team antibullismo attraverso apposita procedura che definisce l'istituto (mail ad hoc, tramite gli uffici e postazioni specifiche, etc...).

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

### **Strumenti a disposizione di studenti/esse**

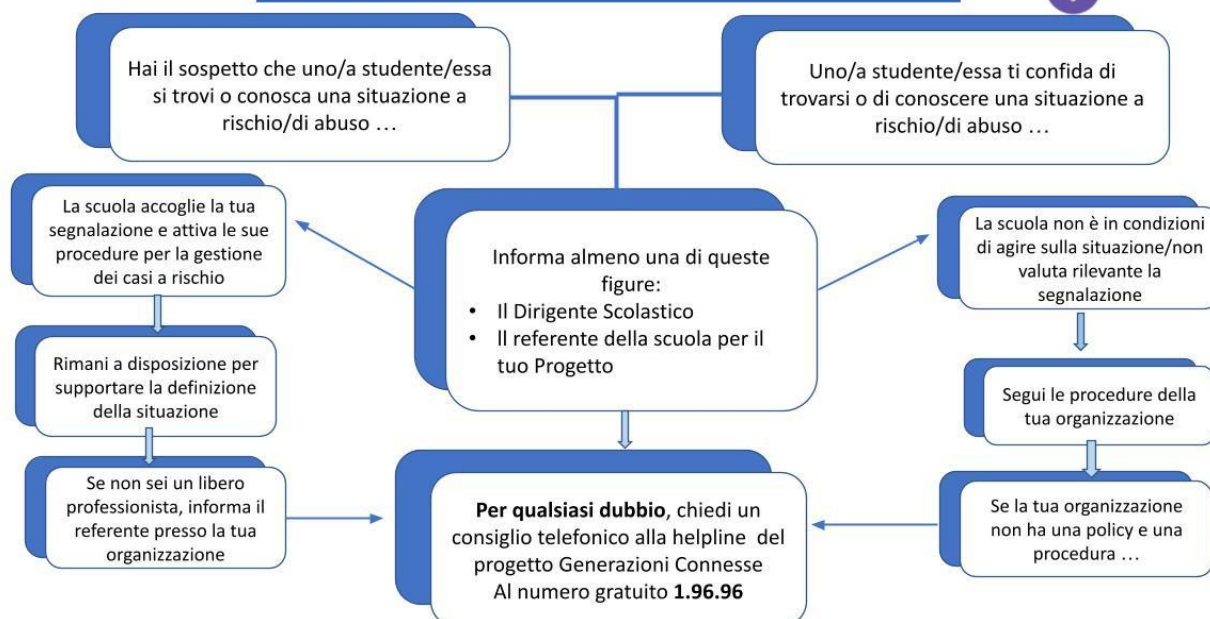
Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione: un indirizzo e-mail specifico per le segnalazioni; scatola/box per la raccolta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

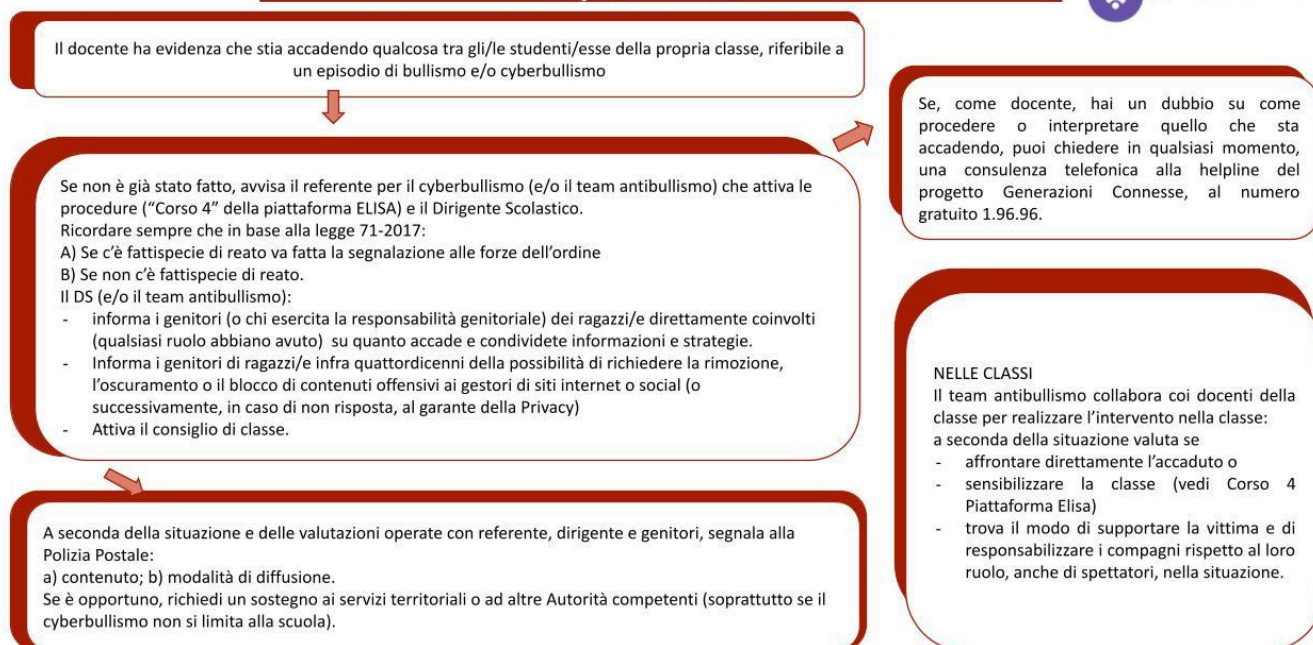
Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle [Linee di Orientamento per la prevenzione e il contrasto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

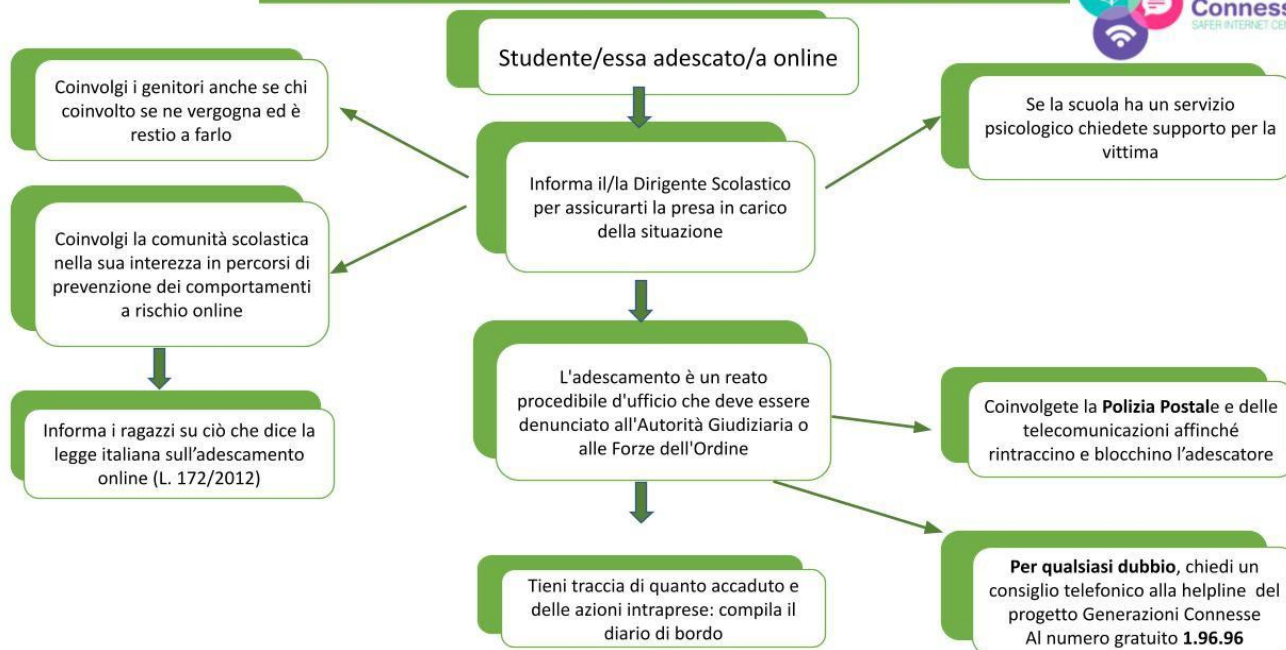




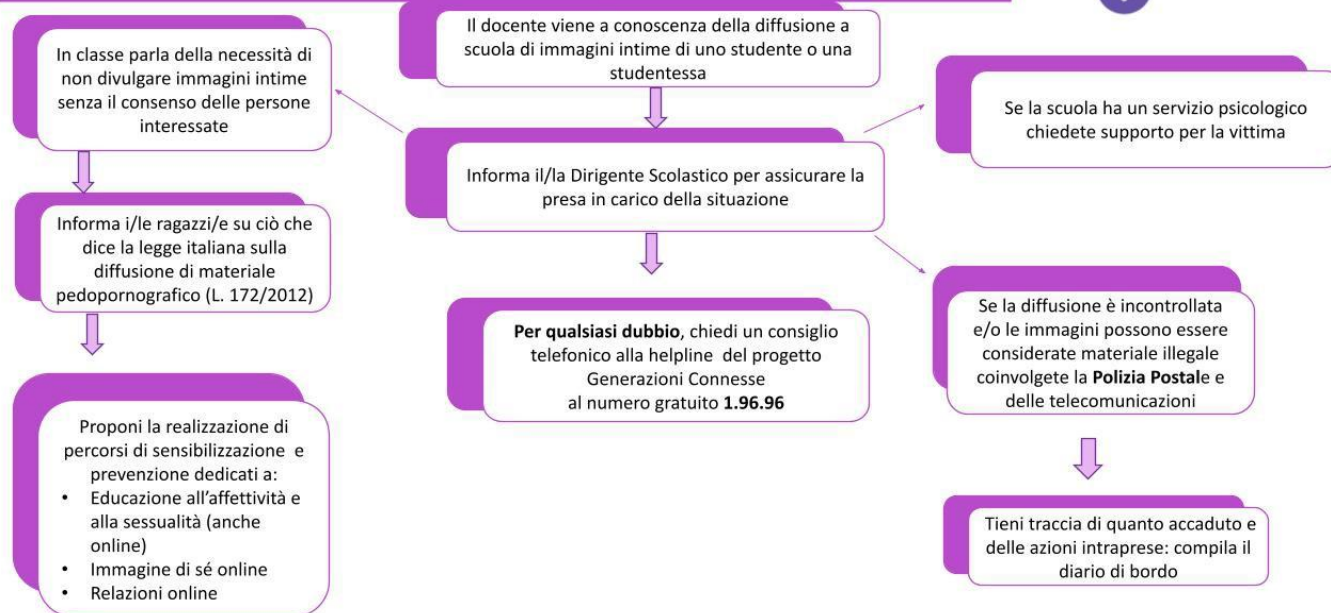
## Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



## Procedure interne: cosa fare in caso di Adescamento Online?



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



### Was bedeutet das für unsere Schule?

Das Technische Institut Cesare Battisti in Bozen stellt unserer Schulgemeinschaft „BattBull“ zur Verfügung, eine innovative App, die intern vom Technischen Institut Cesare Battisti in Bozen entwickelt wurde. Die App entspricht den Datenschutzbestimmungen und ist das wichtigste Instrument zur Prävention und Bekämpfung von Mobbing und Cybermobbing.

- **Zweck der App:** Die Anwendung ist ein direkter und sicherer Kanal, um Fälle von Mobbing, Verdachtsfälle von Notlagen oder unangemessenes Verhalten zu melden, die online oder in der Schule stattgefunden haben.
- **Meldevorgang:** Die Schüler können Meldungen anonym oder unter Angabe ihres Namens einreichen. Die Informationen gehen ausschließlich an den Schulleiter und den Mobbing-Beauftragten, wodurch höchste Vertraulichkeit gewährleistet ist.
- **Zugänglichkeit und Registrierung:** Alle Schüler und Mitarbeiter sind eingeladen, die App auf ihren Geräten zu installieren (auch im BYOD-Modus), um ein weitreichendes und aktives Schutznetzwerk zu schaffen.
- **Pädagogisches Ziel:** Die BattBull-App ist nicht nur ein Kontrollinstrument, sondern ein Mittel, um Schüler zu befähigen, indem jeder Nutzer zu einem aktiven Beobachter wird, der zum gemeinsamen Wohlbefinden beiträgt.
- **Datenverarbeitung:** Die Anwendung ist geprüft und hält sich strikt an die Vorschriften zum Schutz personenbezogener Daten, im Einklang mit dem Datenschutzkonzept der Schule.