



*Ministero dell'Istruzione, dell'Università e della Ricerca*

Dipartimento per il sistema educativo di istruzione e  
di formazione

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

**Aggiornamento**

**LINEE DI ORIENTAMENTO**

**per la prevenzione e il contrasto del cyberbullismo**

**Ottobre 2017**



*Ministero dell'Istruzione, dell'Università e della Ricerca*

## Dipartimento per il sistema educativo di istruzione e di formazione

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

### Indice

#### Premessa

#### **1. Interventi per la prevenzione e il contrasto del fenomeno**

**1.1 L'iniziativa *Generazioni connesse* e altri strumenti utili per un uso corretto e consapevole delle tecnologie digitali**

#### **2. Modalità di segnalazione di situazioni e/o comportamenti a rischio**

#### **3. *Governance*: una nuova organizzazione**

**3.1 Azioni mirate delle scuole rivolte agli studenti e alle loro famiglie: il ruolo del Dirigente scolastico e del docente referente**

#### **4. Nuovi strumenti introdotti dalla L. 71/2017: l'ammonimento**



*Ministero dell'Istruzione, dell'Università e della Ricerca*

## Dipartimento per il sistema educativo di istruzione e di formazione

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

### **Premessa**

Il presente testo ha lo scopo di dare continuità alle Linee di orientamento emanate nell'aprile del 2015, apportando le integrazioni e le modifiche necessarie in linea con i recenti interventi normativi<sup>1</sup>, con particolare riferimento alle innovazioni introdotte con l'emanazione della L. 71/2017: "*Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo*". Lo stesso è, quindi, da intendersi quale strumento flessibile e suscettibile di periodici aggiornamenti<sup>2</sup>, tale da rispondere alle sfide educative e pedagogiche derivanti dall'evolversi costante e veloce delle nuove tecnologie.

La Legge 71/2017 si presenta con un approccio inclusivo e invita diversi soggetti a sviluppare una progettualità volta alla prevenzione e al contrasto del cyberbullismo, secondo una prospettiva di intervento educativo e mai punitivo, prevedendo all'art.3 l'istituzione di un Tavolo di lavoro, presso la Presidenza del Consiglio dei Ministri, coordinato dal MIUR, con il compito di redigere un piano di azione integrato e realizzare un sistema di raccolta di dati per il monitoraggio, avvalendosi anche della collaborazione della Polizia Postale e delle Comunicazioni e delle altre Forze di polizia.

Tale piano sarà integrato con un codice di co-regolamentazione per la prevenzione e il contrasto del cyberbullismo a cui dovranno attenersi gli operatori che forniscono servizi di social networking e tutti gli altri operatori della rete Internet; con il predetto codice sarà istituito un comitato di monitoraggio con il compito di definire gli standard per l'istanza di oscuramento di cui all'articolo 2, comma 1, della Legge 71/2017.

---

<sup>1</sup> Art.1, commi 7, 57,58 della Legge n.107 del 15 luglio 2015 "Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti"; Legge n. 71 del 29 maggio 2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo".

<sup>2</sup>L' articolo 4, comma 1 della Legge 71 del 29 maggio 2017 prevede che l'aggiornamento delle Linee di orientamento avvenga con cadenza biennale.



*Ministero dell'Istruzione, dell'Università e della Ricerca*

## Dipartimento per il sistema educativo di istruzione e di formazione

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Il Piano dovrà stabilire, altresì, le iniziative di informazione e di prevenzione del cyberbullismo con il coinvolgimento dei servizi socio-educativi territoriali, in sinergia con le scuole, anche attraverso periodiche campagne informative, di prevenzione e di sensibilizzazione avvalendosi dei media, degli organi di comunicazione, di stampa e di enti privati.

Il dettato normativo attribuisce, quindi, a una pluralità di soggetti compiti e responsabilità ben precisi, ribadendo il ruolo centrale della Scuola che è chiamata a realizzare azioni in un'ottica di *governance* diretta dal MIUR che includano “la *formazione del personale, la partecipazione di un proprio referente per ogni autonomia scolastica, la promozione di un ruolo attivo degli studenti, nonché di ex studenti che abbiano già operato all'interno dell'istituto scolastico in attività di peer education, la previsione di misure di sostegno e di rieducazione dei minori coinvolti*”.<sup>3</sup> Sentito il Dipartimento per la Giustizia Minorile e di Comunità (DGMC), il MIUR adotta le presenti linee di orientamento per la prevenzione ed il contrasto del cyberbullismo nelle scuole.

Centrale risulta la figura del docente referente che la scuola individua preferibilmente tra i docenti che posseggano competenze specifiche ed abbiano manifestato l'interesse ad avviare un percorso di formazione specifico.

Il referente diventa, così, l'interfaccia con le forze di Polizia, con i servizi minorili dell'amministrazione della Giustizia, le associazioni e i centri di aggregazione giovanile sul territorio, per il coordinamento delle iniziative di prevenzione e contrasto del cyberbullismo.

Nelle more, quindi, della costituzione e dell'operatività del Tavolo inter-istituzionale presso la Presidenza del Consiglio dei Ministri, le presenti linee di orientamento rappresentano un primo strumento che potrà essere utile a orientare le azioni che le scuole vorranno autonomamente intraprendere, e che saranno successivamente integrate in un complessivo Piano di Azione nazionale.

### ***1. Interventi per la prevenzione e contrasto del fenomeno del cyberbullismo.***

---

<sup>3</sup> Art. 4, comma. 2 della Legge n. 71 del 29 maggio 2017.



*Ministero dell'Istruzione, dell'Università e della Ricerca*

## Dipartimento per il sistema educativo di istruzione e di formazione

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

La Legge 107 del 2015<sup>4</sup> ha introdotto, tra gli obiettivi formativi prioritari, lo sviluppo delle competenze digitali degli studenti, finalizzato anche a un utilizzo critico e consapevole dei social network e dei media, e declinato dal Piano Nazionale Scuola Digitale.<sup>5</sup>

Le studentesse e gli studenti devono essere sensibilizzati ad un uso responsabile della Rete e resi capaci di gestire le relazioni digitali in *agorà* non protette. Ed è per questo che diventa indispensabile la maturazione della consapevolezza che Internet può diventare, se non usata in maniera opportuna, una pericolosa forma di dipendenza. Compito della Scuola è anche quello di favorire l'acquisizione delle competenze necessarie all'esercizio di una cittadinanza digitale consapevole. Responsabilizzare le alunne e gli alunni significa, quindi, mettere in atto interventi formativi, informativi e partecipativi. Tale principio è alla base dello Statuto delle studentesse e degli studenti<sup>6</sup> che sottolinea la finalità educativa anche quando si rendano necessari provvedimenti disciplinari, comunque tesi a ripristinare comportamenti corretti all'interno dell'istituto *“attraverso attività di natura sociale e culturale ed in generale a vantaggio della comunità scolastica”*.

Nel corso degli ultimi anni, inoltre, il MIUR ha siglato Protocolli di Intesa e avviato collaborazioni con le più importanti Istituzioni e Associazioni che, a vario titolo, si occupano di prevenzione e contrasto del bullismo e cyberbullismo al fine di creare un'alleanza e una convergenza di strumenti e risorse atti a rispondere alla crescente richiesta di aiuto da parte delle istituzioni scolastiche e delle famiglie<sup>7</sup>.

### ***1.1. L'iniziativa Generazioni connesse e altri strumenti utili per un uso corretto e consapevole delle tecnologie digitali.***

---

<sup>4</sup> Art. 1, commi 57, 58.

<sup>5</sup> <http://www.miur.gov.it/web/guest/scuola-digitale>

<sup>6</sup> Art. 4, comma 2., D.P.R. 24 giugno 1998, n. 249.

<sup>7</sup> Nell'ottica della collaborazione inter-istituzionale che deve caratterizzare le attività dell'amministrazione centrale e periferica e delle stesse istituzioni scolastiche, si auspica un'azione sinergica con le strutture centrali e territoriali del Dipartimento per la Giustizia Minorile e di Comunità che ha previsto, nella propria riorganizzazione, uno specifico ufficio per la prevenzione della devianza e per la giustizia riparativa.



*Ministero dell'Istruzione, dell'Università e della Ricerca*

## Dipartimento per il sistema educativo di istruzione e di formazione

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Per promuovere strategie finalizzate a rendere Internet un luogo più sicuro per gli utenti più giovani, favorendone un uso positivo e consapevole, il MIUR ha avviato l'iniziativa “*Generazioni Connesse*”, sostenuta dalla Commissione Europea<sup>8</sup>, con lo scopo di fornire alle istituzioni scolastiche una serie di strumenti didattici, di immediato utilizzo, tra cui:

- attività di formazione (online e in presenza) rivolte in maniera specifica alle comunità scolastiche (insegnanti, bambini/e, ragazzi/e, genitori, educatori) che intraprenderanno un percorso dedicato;

- attività di informazione e sensibilizzazione realizzate in collaborazione con la Polizia di Stato per approfondire i temi della navigazione sicura in Rete.

Le scuole che intendano partecipare all'iniziativa possono collegarsi all'indirizzo [www.generazioniconnesse.it](http://www.generazioniconnesse.it) e seguire le istruzioni riportate per effettuare l'iscrizione al progetto.

Attraverso un iter guidato e materiali specifici di lavoro, le scuole iscritte a *Generazioni connesse*, intraprendono un percorso per far emergere i punti di forza e di debolezza dell'istituto stesso, sulle tematiche connesse al Progetto, mediante la compilazione di un questionario di autovalutazione disponibile sul sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it). Il questionario è uno strumento che consente all'istituto di identificare i propri bisogni, le aree di miglioramento e le azioni da intraprendere per giungere all'elaborazione di un progetto personalizzato denominato “Piano d'azione”.

Tale Piano<sup>9</sup> consentirà alle istituzioni scolastiche di focalizzare il proprio Piano Triennale dell'Offerta Formativa al fine di definire:

- il proprio approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica;

- le norme comportamentali e le procedure per l'utilizzo delle tecnologie dell'informazione e della comunicazione (ICT) in ambiente scolastico;

- le misure per la prevenzione;

---

<sup>8</sup> L'iniziativa è coordinata dal MIUR e realizzata in partenariato con: Ministero dell'Interno-Polizia Postale e delle Comunicazioni, l'Autorità Garante per l'Infanzia e l'Adolescenza, Save the Children Italia Onlus, Sos Il Telefono Azzurro, l'Università degli Studi di Firenze, l'Università degli Studi di Roma “La Sapienza”, Skuola.net, la Cooperativa E.D.I., Movimento Difesa del Cittadino e l'Agenzia Dire.

<sup>9</sup> <http://www.generazioniconnesse.it/site/it/area-scuole/>



*Ministero dell'Istruzione, dell'Università e della Ricerca*

## Dipartimento per il sistema educativo di istruzione e di formazione

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

- le misure per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali;

Il percorso è rivolto alle classi quarta e quinta della scuola primaria e a tutte le classi della scuola secondaria di primo grado.

Per la realizzazione del “Piano d’azione”, l’istituto scolastico è affiancato da un servizio di “supporto scuole” (supportoscuole@generazioniconnesse.it) e da personale qualificato del Safer Internet Centre italiano.

Un ulteriore strumento per contrastare comportamenti dannosi online e allo stesso tempo accrescere la conoscenza del fenomeno è “iGloss@ 1.1<sup>10</sup>, l’Abc dei comportamenti devianti online”, elaborato dal Dipartimento per la Giustizia Minorile e di Comunità.

Il glossario, nella ricognizione dei termini specialistici sui comportamenti online a rischio, offre una sintetica spiegazione delle principali caratteristiche delle condotte devianti e dei risvolti socio-giuridici.

L’obiettivo non è esclusivamente descrivere e inquadrare i nuovi fenomeni della devianza online, ma favorire, altresì, l’acquisizione di consapevolezza sulle conseguenze sociali e giudiziarie di queste specifiche trasgressioni.

Il glossario, disponibile online in lingua italiana e inglese sul sito del Ministero della Giustizia ([www.giustizia.it](http://www.giustizia.it)), è rivolto a operatori dei servizi sociali, sanitari, giudiziari, giovani e loro genitori.

#### **4. Modalità di segnalazione di situazioni e/o comportamenti a rischio**

La Legge 71/2017 indica per la prima volta tempi e modalità per richiedere la rimozione di contenuti ritenuti dannosi per i minori. L’art.2, infatti, prevede che il minore di quattordici anni, ovvero il genitore o altro soggetto esercente la responsabilità sul minore che abbia subito un atto di cyberbullismo, può inoltrare un’istanza per l’oscuramento, la rimozione o il blocco di qualsiasi dato personale del minore, diffuso nella rete:

---

<sup>10</sup>Le informazioni sono reperibili al sito: [https://www.giustizia.it/giustizia/it/mg\\_2\\_5\\_12.page](https://www.giustizia.it/giustizia/it/mg_2_5_12.page)



*Ministero dell'Istruzione, dell'Università e della Ricerca*

## Dipartimento per il sistema educativo di istruzione e di formazione

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

- ✓ al titolare del trattamento
- ✓ al gestore del sito internet
- ✓ al gestore del social media

Infatti, se entro ventiquattro ore dal ricevimento dell'istanza i soggetti responsabili non abbiano comunicato di avere preso in carico la segnalazione, e entro quarantotto ore provveduto, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante<sup>11</sup> per la protezione dei dati personali, il quale provvede entro quarantotto ore dal ricevimento della richiesta.

Le scuole possono, altresì, segnalare episodi di cyberbullismo e la presenza di materiale pedopornografico on line al servizio *Helpline* di Telefono Azzurro 1.96.96, una piattaforma integrata che si avvale di telefono, chat, sms, whatsapp e skype -strumenti per aiutare i ragazzi e le ragazze a comunicare il proprio disagio-e alla *Hotline* "Stop-It" di Save the Children, all'indirizzo [www.stop-it.it](http://www.stop-it.it), che consente agli utenti della Rete di segnalare la presenza di materiale pedopornografico<sup>12</sup> online. Attraverso procedure concordate, le segnalazioni sono successivamente trasmesse al Centro Nazionale per il Contrasto alla Pedopornografia su Internet, istituito presso la Polizia Postale e delle Comunicazioni, per consentire le attività di investigazione necessarie.

### **3 Governance: una nuova organizzazione.**

In linea con quanto previsto dalla Legge 71/2017, il MIUR ha intrapreso una riorganizzazione della struttura amministrativa centrale e periferica che opera per la prevenzione del cyberbullismo, nella convinzione che la migliore modalità di intervento passi attraverso l'istituzione di un efficace sistema di *governance* che coinvolga le istituzioni, la società civile, gli adulti e gli stessi minori.

È stato introdotto un nuovo sistema di *governance* che parte dalla costituzione di un Tavolo tecnico centrale, previsto dall'art. 3 della L. 71/2017 e di prossima costituzione, di cui faranno parte istituzioni, associazioni, operatori di social networking e della rete internet, fino a giungere alla

---

<sup>11</sup>Il Garante ha predisposto il modello per la segnalazione di casi di cyberbullismo che si trova sul sito <http://www.garanteprivacy.it/cyberbullismo>.

<sup>12</sup> Per la legislazione corrente, anche il materiale prodotto attraverso la pratica del *sexting*, che abbiamo visto essere molto diffusa tra i giovani, è da considerarsi pedopornografico.



*Ministero dell'Istruzione, dell'Università e della Ricerca*

## Dipartimento per il sistema educativo di istruzione e di formazione

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

richiesta dell'individuazione, nel rispetto dell'autonomia, di un docente referente per ogni istituzione scolastica.

Nelle more della costituzione di detto Tavolo di coordinamento nazionale, rimane e rimarrà fondamentale l'importante azione di coordinamento territoriale esercitata dagli Uffici Scolastici Regionali, per il tramite degli Osservatori Regionali all'uopo istituiti e al supporto della rete locale dei Centri Territoriali. La Legge richiama, infine, ad un'ulteriore azione di raccordo con ulteriori figure professionali, altri Enti e istituzioni deputati alla prevenzione e al contrasto del cyberbullismo quali assistenti sociali, educatori, operatori della Giustizia minorile.

### ***3.1 Azioni mirate delle scuole e rivolte agli studenti e alle loro famiglie: il ruolo del dirigente scolastico e del docente referente***

La L. 71/2017 all'art. 5 prevede che, nell'ambito della promozione degli interventi finalizzati ad assicurare la qualità dei processi formativi e la collaborazione delle risorse culturali, professionali, sociali del territorio, il dirigente scolastico, definisca le linee di indirizzo del Piano Triennale dell'Offerta Formativa (PTOF) e del Patto di Corresponsabilità (D.P.R. 235/07) affinché contemplino misure specificatamente dedicate alla prevenzione del cyberbullismo<sup>13</sup>.

Le misure di intervento immediato che i dirigenti scolastici sono chiamati a effettuare, qualora vengano a conoscenza di episodi di cyberbullismo, dovranno essere integrate e previste nei Regolamenti di Istituto e nei Patti di Corresponsabilità, al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione.

Sarà cura del dirigente assicurare la massima informazione alle famiglie di tutte le attività e iniziative intraprese, anche attraverso una sezione dedicata sul sito web della scuola, che potrà rimandare al sito del MIUR [www.generazioniconnesse.it](http://www.generazioniconnesse.it) per tutte le altre informazioni di carattere generale.

---

<sup>13</sup> Il comma 1 dell'art. 5 prevede che il dirigente scolastico, "salvo che il fatto costituisca reato, in applicazione della normativa vigente e delle disposizioni di cui al comma 2, il dirigente scolastico che venga a conoscenza di atti di cyberbullismo ne informa tempestivamente i soggetti esercenti la responsabilità genitoriale ovvero i tutori dei minori coinvolti e attiva adeguate azioni di carattere educativo".



*Ministero dell'Istruzione, dell'Università e della Ricerca*

## Dipartimento per il sistema educativo di istruzione e di formazione

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Parimenti è auspicabile che il dirigente scolastico attivi specifiche intese con i servizi territoriali (servizi della salute, servizi sociali, forze dell'ordine, servizi minorili dell'amministrazione della Giustizia) in grado di fornire supporto specializzato e continuativo ai minori coinvolti ove la scuola non disponga di adeguate risorse.

Secondo la stessa logica, la L. 71/2017 prevede che presso ciascuna istituzione scolastica venga individuato un docente referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio.<sup>14</sup>

Nell'ambito dell'istituzione scolastica il docente referente potrà, quindi, svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Ai docenti referenti, così come ai dirigenti scolastici, non sono quindi attribuite nuove responsabilità o ulteriori compiti, se non quelli di raccogliere e diffondere le buone pratiche educative, organizzative e azioni di monitoraggio, favorendo così l'elaborazione di un modello di e-policy d'istituto.

Tuttavia, al fine assicurare a tutti i soggetti coinvolti in azioni di prevenzione del cyberbullismo strumenti utili per conoscere e attivare azioni di contrasto al fenomeno, il MIUR elaborerà una piattaforma per la formazione dei docenti referenti. Tale azione sarà rafforzata dalle iniziative che saranno previste dal Piano Integrato di cui all'art. 3 della L. 71/2017 nonché dalle iniziative intraprese sia dagli Uffici Scolastici Regionali che dalle istituzioni medesime.

### **5. Nuovi strumenti introdotti dalla L. 71/2017: l'ammonimento**

Nell'ottica di favorire l'anticipo della soglia di sensibilità al rischio e promuovere forme conciliative che possano evitare il coinvolgimento dei minori, sia quali autori del reato sia quali vittime in procedimenti penali, l'art. 7 della Legge 71/2017 prevede uno strumento d'intervento

---

<sup>14</sup> Art. 4, comma 3 della Legge n. 71 del 29 maggio 2017.



*Ministero dell'Istruzione, dell'Università e della Ricerca*

## Dipartimento per il sistema educativo di istruzione e di formazione

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

preventivo, già sperimentato in materia di atti persecutori (*stalking*), ovvero l'ammonimento del Questore.

Tale previsione risulta pienamente coerente con la scelta legislativa di contrastare il fenomeno del cyberbullismo con azioni di tipo educativo, stimolando nel minore ultraquattordicenne una riflessione sul disvalore sociale del proprio atto nonché una generale presa di coscienza sul medesimo.

Nello specifico, nel caso in cui non si ravvisino reati perseguibili d'ufficio o non sia stata formalizzata querela o presentata denuncia per le condotte di ingiuria (reato recentemente depenalizzato), diffamazione, minaccia o trattamento illecito dei dati personali commessi mediante la rete Internet nei confronti di altro minore, è possibile rivolgere al Questore, autorità provinciale di Pubblica Sicurezza, un'istanza di ammonimento nei confronti del minore ultraquattordicenne autore della condotta molesta. La richiesta potrà essere presentata presso qualsiasi ufficio di Polizia e dovrà contenere una dettagliata descrizione dei fatti, delle persone a qualunque titolo coinvolte ed eventuali allegati comprovanti quanto esposto.

E' bene sottolineare che l'ammonimento, in quanto provvedimento amministrativo, non richiede una prova certa e inconfutabile dei fatti, essendo sufficiente la sussistenza di un quadro indiziario che garantisca la verosimiglianza di quanto dichiarato.

Qualora l'istanza sia considerata fondata, anche a seguito degli approfondimenti investigativi ritenuti più opportuni, il Questore convocherà il minore responsabile insieme ad almeno un genitore o ad altra persona esercente la potestà genitoriale, ammonendolo oralmente e invitandolo a tenere una condotta conforme alla legge con specifiche prescrizioni che, ovviamente, varieranno in base ai casi.

La legge non prevede un termine di durata massima dell'ammonimento ma specifica che i relativi effetti cesseranno al compimento della maggiore età.

Pur non prevedendo un'aggravante specifica per i reati che il minore potrà compiere successivamente al provvedimento di ammonimento, senza dubbio tale strumento rappresenta un



*Ministero dell'Istruzione, dell'Università e della Ricerca*

## Dipartimento per il sistema educativo di istruzione e di formazione

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

significativo deterrente per incidere in via preventiva sui minori ed evitare che comportamenti, frequentemente assunti con leggerezza, possano avere conseguenze gravi per vittime e autori.

Firmato digitalmente da FEDELI VALERIA  
C = IT  
O = MINISTERO ISTRUZIONE UNIVERSITA' E  
RICERCA/80185250588



# *Ministero dell'Istruzione*

*Dipartimento per il sistema educativo di istruzione e di formazione*

*Direzione Generale per lo Studente, l'Inclusione e l'Orientamento scolastico*

**Ai Direttori Generali degli  
Uffici Scolastici Regionali  
LORO SEDI**

**Alla Provincia Autonoma di Trento  
Servizio istruzione – TRENTO**

**All'Intendenza scolastica per la lingua  
italiana – BOLZANO**

**All'Intendenza scolastica per la lingua  
tedesca – BOLZANO**

**All'Intendenza scolastica per la lingua  
ladina – BOLZANO**

**Al Sovrintendente Scolastico per la Regione Valle d'Aosta  
AOSTA**

**E p.c. Al Capo Dipartimento per il Sistema educativo  
di Istruzione e di Formazione**

**Ai Dirigenti scolastici delle Istituzioni  
scolastiche di ogni grado**

**Ai referenti regionali del bullismo e cyberbullismo (1.71/2017)**

**Ai Referenti regionali per le Consulte  
Provinciali degli Studenti  
Ai Coordinatori regionali dei presidenti  
delle consulte provinciali**

**al Forum delle associazioni dei Genitori**

**al Forum delle associazioni degli Studenti**

**Oggetto: Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo  
- aggiornamento 2021 - per le istituzioni scolastiche di ogni grado.**

Il Ministero dell'Istruzione è impegnato da alcuni anni sull'approfondimento delle strategie di prevenzione e contrasto dei fenomeni di bullismo e del *cyberbullismo* nella comunità scolastica, proprio al fine di intercettare e arginare comportamenti a rischio, temi particolarmente delicati se si considera il contesto reso ancor più complesso dall'emergenza pandemica e conseguenti condizioni di isolamento.

Ufficio II Dirigente: Leonardo Filippone	06/5849 2125 – 2126 <a href="mailto:dgsip.ufficio2@istruzione.it">dgsip.ufficio2@istruzione.it</a>
---	---



# Ministero dell'Istruzione

Dipartimento per il sistema educativo di istruzione e di formazione

Direzione Generale per lo Studente, l'Inclusione e l'Orientamento scolastico

Il legislatore è intervenuto a più riprese, si consideri quanto già previsto dalla L. 107 del 2015 che ha introdotto, tra gli obiettivi formativi prioritari, lo sviluppo delle competenze digitali degli studenti, finalizzato tra l'altro ad un utilizzo critico e consapevole dei social network e dei media, e declinato dal Piano Nazionale Scuola Digitale.

Tale *ratio legis* permea anche la più recente Legge 20 agosto 2019 n. 92 *Introduzione dell'insegnamento scolastico dell'educazione civica* che prevede nell'ambito dell'insegnamento trasversale dell'educazione civica uno specifico approfondimento sull'educazione alla cittadinanza digitale.

Nello specifico, la Legge n.71 del 2017 ha sancito l'obiettivo strategico per il paese di contrastare il fenomeno del *cyberbullismo* in tutte le sue manifestazioni, con azioni a carattere preventivo e con una strategia di attenzione, tutela ed educazione nei confronti dei minori coinvolti, sia nella posizione di vittime sia in quella di responsabili di illeciti, assicurando l'attuazione degli interventi senza distinzione di età nell'ambito delle istituzioni scolastiche.

Nel richiamo dei principi normativi sinteticamente ripercorsi è stato possibile elaborare nel 2017 le prime linee di Orientamento aggiornate con ulteriore documento del 2021 allegato alla presente.

L'intento delle linee guida è consentire ai dirigenti, docenti ed operatori scolastici di comprendere, ridurre e contrastare i fenomeni negativi che colpiscono i nostri studenti, ricorrendo a sollecitazioni e strumenti talora di comprovata evidenza scientifica.

Le accennate linee guida del 2017 hanno consentito lo sviluppo di alcune strategie aventi un primo significativo impatto sulla prevenzione contrasto dei fenomeni. Ad esempio si è resa possibile la creazione di una specifica Piattaforma ELISA (E-learning degli Insegnanti sulle Strategie Antibullismo; [www.piattaformaelisa.it](http://www.piattaformaelisa.it) realizzato in collaborazione con l'Università degli Studi di Firenze) che consente un percorso di formazione gratuita, avviato dal 2018, rivolto ai docenti referenti in materia di bullismo e cyberbullismo incardinati presso le diverse istituzioni scolastiche per l'acquisizione di utili competenze psico-pedagogiche e sociali. I docenti iscritti ad oggi sono più di 5000, mentre le istituzioni scolastiche coinvolte, con uno o due referenti, risultano essere più di 4.000.

Le politiche di intervento sono altresì in linea con le iniziative di matrice europea sul tema, basti citare esemplificativamente il progetto "*Generazioni Connesse - Safer Internet Centre Italiano*", co-finanziato dalla Commissione Europea in partenariato con alcune delle principali realtà italiane che si occupano di sicurezza in Rete: Polizia Postale e delle Comunicazioni, Autorità Garante per l'Infanzia e l'Adolescenza, MIBACT, Save the Children Italia, Telefono Azzurro, EDI onlus, , Università degli Studi di Firenze, Università degli Studi di Roma "La Sapienza", Agenzia Dire, Skuola.Net e l'Ente Autonomo Giffoni Experience.

Generazioni Connesse (cfr [www.generazioniconnesse.it](http://www.generazioniconnesse.it) ) opera su diversi profili, quali: la realizzazione di programmi di educazione e sensibilizzazione sull'utilizzo sicuro di Internet (rivolti a bambini e adolescenti, genitori, insegnanti, educatori e spesso con la partecipazione attiva degli studenti sin dalla fase della progettazione di iniziative divulgative); webinar di approfondimenti su particolari aspetti come ad esempio la individuazione e metodi di segnalazione di fake news o altri comportamenti a rischio; helplines dedicate, per supportare gli utenti su problematiche legate alla Rete, nonché per segnalare la presenza online di materiale pedopornografico.

Le esperienze maturate sul campo, grazie al prezioso impegno delle istituzioni scolastiche, hanno agevolato l'ulteriore aggiornamento presente nell'allegato documento, elaborato anche grazie ai contributi dei Referenti Regionali per il contrasto dei fenomeni di Bullismo e Cyberbullismo, del Forum Studenti e del FONAGS.

Ufficio II  
Dirigente: Leonardo Filippone

06/5849 2125 – 2126  
[dgsip.ufficio2@istruzione.it](mailto:dgsip.ufficio2@istruzione.it)



# Ministero dell'Istruzione

*Dipartimento per il sistema educativo di istruzione e di formazione*

*Direzione Generale per lo Studente, l'Inclusione e l'Orientamento scolastico*

Le Linee di Orientamento 2021 - in continuità con il documento del 2017 e nel richiamo degli interventi prefigurati nella citata L. 71/2017 - nel rispetto del principio di autonomia organizzativo-didattica delle istituzioni scolastiche possono essere un agevole strumento di lavoro per tutti gli operatori del mondo della scuola e della sanità e per quanti a vario titolo si trovano a dover affrontare le problematiche afferenti al disagio giovanile che molto spesso si manifesta attraverso episodi di bullismo e cyberbullismo.

Si indicano di seguito in estrema sintesi i principali punti innovativi delle Linee di Orientamento 2021 rispetto alla versione precedente del 2017:

- Indicazione di strumenti utili e buone pratiche per contrastare i fenomeni del bullismo e cyberbullismo;
- Focus sul Progetto Safer Internet Centre-Generazioni Connesse;
- Analisi degli aspetti relativi alla formazione in modalità e-learning dei docenti referenti (Piattaforma ELISA - E-learning degli Insegnanti sulle Strategie Anti bullismo);
- Indicazioni di procedure operative per elaborare azioni efficaci, individuate a loro volta, in “prioritarie” e “consigliate”;
- Possibili modelli di prevenzione su più livelli (universale-selettiva e indicata) ed esempi di implementazione degli stessi;
- Invito a costituire Gruppi di Lavoro (Team Antibullismo e Team per l’Emergenza) a livello scolastico e territoriale, integrati all’occorrenza da figure specialistiche di riferimento, ricorrendo ad eventuali reti di scopo;
- Suggerimenti di protocolli d’intervento per un primo esame dei casi d’emergenza;
- Ricognizione delle iniziative e impegni degli organi collegiali e del personale scolastico;
- Uso di spazi web dedicati sui siti scolastici istituzionali in ottica di diffusione e rilancio della cultura del rispetto dell’altro;
- Appendice con modello fac-simile di segnalazione di reato o situazioni di rischio ad altri organi competenti.

Nell’auspicio che tale attività sia di effettiva utilità per l’intera comunità scolastica e soprattutto per studenti e famiglie, si confida nella consueta collaborazione degli UU.SS.RR nell’assumere ogni iniziativa ritenuta idonea per una efficace diffusione delle allegate LINEE DI ORIENTAMENTO.

Cordialmente,

**IL DIRETTORE GENERALE**

Antimo PONTICIELLO

Firmato digitalmente da PONTICIELLO  
ANTIMO  
C=IT  
O=MINISTERO ISTRUZIONE UNIVERSITA'  
E RICERCA

Ufficio II  
Dirigente: Leonardo Filippone

06/5849 2125 – 2126  
[dgsip.ufficio2@istruzione.it](mailto:dgsip.ufficio2@istruzione.it)



# Documento di ePolicy

PVPS05000Q

NICOLO' COPERNICO - PAVIA

VIA VERDI 23/25 - 27100 - PAVIA - PAVIA (PV)

Dott.ssa Paola Donatella Penna

# Capitolo 1 - Introduzione al documento di ePolicy

---

## *1.1 - Scopo dell'ePolicy*

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le “competenze digitali” sono fra le abilità chiave all'interno del [Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente](#) e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

1. l'approccio educativo alle tematiche connesse alle “competenze digitali”, alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
2. le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
3. le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
4. le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

## Argomenti del Documento

### 1. Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità
3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

### 2. Formazione e curriculum

1. Curriculum sulle competenze digitali per gli studenti
2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
4. Sensibilizzazione delle famiglie e Patto di corresponsabilità

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

1. Protezione dei dati personali
2. Accesso ad Internet
3. Strumenti di comunicazione online
4. Strumentazione personale

### 4. Rischi on line: conoscere, prevenire e rilevare

1. Sensibilizzazione e prevenzione
2. Cyberbullismo: che cos'è e come prevenirlo
3. Hate speech: che cos'è e come prevenirlo
4. Dipendenza da Internet e gioco online
5. Sexting
6. Adescamento online
7. Pedopornografia

### 5. 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

## Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi

all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

La E-policy si configura quindi come il documento redatto dal Liceo Copernico per l'adozione e condivisione di:

- Norme e procedure per l'utilizzo consapevole delle TIC nell'ambito della didattica e nell'ambiente scolastico

- Misure per la prevenzione e rilevazione di criticità e per sanzionare comportamenti scorretti che possono insorgere, connessi all'uso delle TIC

Il presente documento è un contributo della referente per la prevenzione del Cyberbullismo, su cui potrà lavorare lo staff dirigenziale nella declinazione degli specifici aggiornamenti previsti. Verrà periodicamente monitorato per l'inserimento delle nuove azioni di contrasto all'uso non corretto delle tecnologie e per la revisione delle azioni intraprese.

Tutte le infrazioni alla e-policy saranno segnalate alla Dirigente scolastica.

## ***1.2 - Ruoli e responsabilità***

Affinché l'E-policy 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.

**Il Dirigente scolastico** garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica ed è informato sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR; promuove inoltre la cultura della sicurezza online e, ove possibile, dà il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Il Dirigente Scolastico ha la responsabilità di gestire ed intervenire

nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

**L'animatore digitale** supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre ad essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); potrebbe, inoltre, monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e avere il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

**Il referente per il bullismo e cyberbullismo:** *“Ogni Istituto scolastico, nell’ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo”* (Art. 4 Legge n.71/2017, “Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo” (permalink – file 1 LEGGE 71\_2017 in allegato)). Tale figura ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può **avvalersi della collaborazione delle Forze di polizia**, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, in quanto (ove possibile) potrebbe coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori (un approfondimento maggiore sui ruoli relativi alle problematiche del bullismo e del cyberbullismo verrà fornito nel modulo 4, al paragrafo 4.2.).

**I Docenti** hanno un ruolo centrale nel **diffondere la cultura dell'uso responsabile delle TIC e della Rete**. Potrebbero, innanzitutto, integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti dovrebbero accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete; **hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso**, anche online, che vede coinvolti studenti e studentesse.

**Il personale Amministrativo, Tecnico e Ausiliario (ATA)** svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. Diverse figure che in sinergia si occupano, ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico, che passa anche attraverso lo sviluppo della

cultura digitale e dell'organizzazione del tempo scuola. Esiste, cioè, un **concreto coinvolgimento del personale ATA** nell'applicazione della [legge 107/15 \("La Buona Scuola"\)](#) che concerne non solo il tempo scuola e il potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA dovrebbe, all'interno dei singoli regolamenti d'Istituto, **essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo** insieme ad altre figure, e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

**Gli Studenti e le Studentesse** dovrebbero, in relazione al proprio grado di maturità e consapevolezza raggiunte, 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; dovrebbero 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 Genitori**, in continuità con l'Istituto scolastico, dovrebbero essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete nonché sull'uso responsabile dei device personali; dovrebbero relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e 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 dell'Istituto.**

**Gli Enti educativi esterni e le associazioni** che entrano in relazione con la scuola dovrebbero conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; dovrebbero, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme. A tal fine si suggerisce di prevedere una sezione specifica dell'ePolicy con indicazioni ad hoc e procedure standard per gli attori esterni.

Esiste una corresponsabilità educativa e formativa che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse. Si può parlare di **tre tipologie di "culpa"**:

- **culpa in vigilando**: concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (così come da art. 2048 del c.c.). Tale condizione è superabile se ci si avvale di una prova liberatoria di non aver potuto impedire il fatto (recita il terzo comma dell'art. 2048 c.c.: "le persone indicate nei commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto").

- **culpa in organizzando:** si riferisce ai provvedimenti previsti e presi dal Dirigente Scolastico ritenuti come non soddisfacenti e quindi elemento favorevole al verificarsi dell'eventuale incidente.
- **culpa in educando:** fa capo ai genitori i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.

### ***1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto***

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

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

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

La dirigenza e le figure referenti nei vari ambiti (non solo il referente bullismo/cyberbullismo), in maniera condivisa con i docenti, dovrebbero redigere l'informativa per i professionisti esterni, anche dividendola per aree, paragrafi e sottoparagrafi.

A titolo di esempio, e in linea generale, si potrebbe prevedere:

- Premessa e obiettivi dell'informativa.
- Destinatari (organizzazioni e soggetti esterni).
- Ambiti di applicazione (il progetto specifico o delle attività) e Ruoli (individuare i docenti di riferimento del progetto specifico o delle attività).
- Regolamento / Codice di comportamento.
- Procedure di segnalazione (Allegare i moduli di segnalazione per le situazioni di rischio (vedi cap.5 – procedure per soggetti esterni).

- Provvedimenti nel caso di:
  - omessa segnalazione
  - comportamenti in violazione del codice di comportamento.

Una volta individuate le varie aree e tutti gli attori da coinvolgere, è necessario pensare anche alla possibilità di monitorare, aggiornare ed integrare tale documento vincolante fra le parti, che va ufficialmente approvato e sottoscritto dai proponenti istituzionali della scuola. È, inoltre, importante che nel regolamento siano esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Utile anche sottolineare che esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

## ***1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica***

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/le studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

Il presente documento verrà pubblicato sul sito del Liceo Copernico affinché sia reso pubblico.

## ***1.5 - Gestione delle infrazioni alla ePolicy***

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

Le possibili condotte sanzionabili, in relazione all'uso improprio delle TIC e della Rete a scuola da parte degli studenti e delle studentesse, possono essere:

- **la condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie;**
- **la condivisione di scatti intimi e a sfondo sessuale; la condivisione di dati personali; l'invio di immagini o video volti all'esclusione di compagni/e.**

A seconda dell'età dello studente o della studentessa, è molto importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione, allo scopo di promuovere una maggior consapevolezza circa l'utilizzo delle TIC e di Internet.

È opportuno, inoltre, valutare la natura e la gravità di quanto accaduto, al fine di **considerare la necessità di denunciare l'episodio** (con il coinvolgimento ad es. della Polizia Postale) o di garantire immediato supporto psicologico allo/la studente/ssa attraverso i servizi predisposti, qualora ciò fosse necessario.

E' opportuno riflettere anche sulla disciplina del personale scolastico riguardante le possibili infrazioni nelle quali il personale stesso, soprattutto i docenti, può incorrere se utilizza impropriamente i device o la Rete, nonché quelle violazioni che non intervengano nella segnalazione di condotte improprie dei/le propri/ie studenti/studentesse.

## ***1.6 - Integrazione dell'ePolicy con Regolamenti esistenti***

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

## ***1.7 – Monitoraggio dell'implementazione della ePolicy e suo aggiornamento***

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

## **Il nostro piano d'azioni**

### **Azioni da svolgere entro un'annualità scolastica:**

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni

Connesse rivolto ai docenti

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

### **Azioni da svolgere nei prossimi 3 anni:**

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse

sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy

rivolto ai docenti

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

# Capitolo 2 - Formazione e curriculum

## 2.1. Curriculum sulle competenze digitali per gli studenti

---

I ragazzi usano la Rete quotidianamente, talvolta in modo più “intuitivo” ed “agile” rispetto agli adulti, ma non per questo sono dotati di maggiori “competenze digitali”.

Infatti, “la competenza digitale presuppone l’interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l’alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l’alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l’essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico” ([“Raccomandazione del Consiglio europeo relativa alla competenze chiave per l’apprendimento permanente”](#), C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curriculum digitale.

Per progettare il curriculum digitale è possibile seguire i seguenti consigli, chiedendosi:

quali classi coinvolgere? Per quante ore all’anno? Quali obiettivi e temi si ritengono più urgenti da affrontare? Con quali metodologie? Il percorso verrà progettato e portato avanti da docenti interni alla scuola o si pensa di rivolgersi a professionisti esterni? Come si pensa di procedere per la valutazione e il monitoraggio del percorso?

E’ possibile definire meglio i dettagli del curriculum nel piano di azione, anche a partire dagli ulteriori contenuti della e-policy.

Il curriculum sulle competenze digitali che l’Istituto si impegna a progettare e implementare, parte dall’individuazione dei temi ritenuti più importanti e delle classi da coinvolgere (l’ePolicy è un documento che va periodicamente aggiornato in base alle esigenze dell’Istituto).

Le competenze digitali richiamano diverse dimensioni sulle quali sarà possibile lavorare in classe, in un’ottica che integra la dimensione tecnologica con quella cognitiva ed etica (Calvani, Fini e Ranieri 2009):

- **dimensione tecnologica:** è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un’adeguata comprensione della “grammatica” dello strumento.
- **dimensione cognitiva:** fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità.
- **dimensione etica e sociale:** la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone un po’ più l’accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

Tra i documenti più importanti per progettare e implementare un buon curriculum sulle competenze digitali, il DigComp, in particolare, è diventato un riferimento per lo sviluppo e la pianificazione strategica di iniziative sulle competenze digitali, sia a livello europeo sia nei singoli stati membri dell'Unione. Il documento prevede:

1. Aree di competenze individuate come facenti parte delle competenze digitali;
2. Descrittori delle competenze e titoli pertinenti a ciascuna area (21 competenze);
3. Livelli di padronanza per ciascuna competenza (i livelli sono 8);
4. Conoscenze, abilità e attitudini applicabili a ciascuna competenza;
5. Esempi di utilizzo sull'applicabilità della competenza per diversi scopi.

Le aree di competenza individuate dal Digcomp sono, nello specifico:

### **Area 1: “Alfabetizzazione e dati”**

L'area s'inquadra nella dimensione “informazionale” o “cognitiva” delle competenze digitali. Essa è relativa alla capacità di cercare, selezionare, valutare e riprocessare le informazioni in Rete. Nello specifico, per quest'area si dovrebbe puntare a sviluppare in bambini e ragazzi le seguenti competenze: 1. Navigare, ricercare e filtrare dati, informazioni e contenuti digitali; 2. Valutare e gestire dati, informazioni e contenuti digitali; 3. Saper riconoscere e sapersi difendere da contenuti dannosi e pericolosi in Rete (es. app, giochi online, siti non adatti ai minori, materiale pornografico e pedo-pornografico etc.).

### **Area 2: “Comunicazione e collaborazione”**

Quest'area fa riferimento a quelle competenze volte a riconoscere le giuste ed appropriate modalità per comunicare e relazionarsi online: 1. Saper interagire con gli altri attraverso le tecnologie digitali; 2. Essere consapevoli nella condivisione delle informazioni in Rete; 3. Essere buoni “cittadini digitali”; 4. Collaborare adeguatamente con gli altri attraverso le tecnologie digitali; 5. Conoscere le “Netiquette”, ovvero le norme di comportamento online; 6. Saper gestire la propria “identità digitale”.

### **Area 3: “Creazione di contenuti digitali”**

Quest'area fa riferimento alle capacità di “valutare le modalità più appropriate per modificare, affinare, migliorare e integrare nuovi contenuti e informazioni specifici per crearne di nuovi e originali” (cfr. DigComp 2.1.). Le specifiche competenze digitali che andranno sviluppate in questo caso sono: 1. Creare e modificare contenuti digitali in diversi formati per esprimersi attraverso mezzi digitali; 2. Modificare, affinare, migliorare e integrare informazioni e contenuti all'interno di un corpus di conoscenze esistente per creare conoscenze e contenuti nuovi, originali e rilevanti; 3. Capire come il copyright e le licenze si applicano ai dati, alle informazioni e ai contenuti digitali.

### **Area 4: “Sicurezza”**

Quest'area è parte di una dimensione più generale definita come “benessere digitale” che include la necessità di salvaguardare i propri dati personali e rispettare le regole nel trattare i dati altrui. Nello specifico, bisognerebbe puntare a sviluppare in bambini e ragazzi le seguenti competenze: 1. Imparare a proteggere i dispositivi e i contenuti digitali e comprendere i rischi e le minacce presenti negli ambienti digitali. Conoscere le misure di sicurezza e protezione e tenere in debita considerazione l'affidabilità e la privacy; 2. Proteggere i dati personali e la privacy negli ambienti digitali. Capire come utilizzare e condividere informazioni personali proteggendo se stessi e gli altri dai danni. Comprendere che i servizi digitali hanno un “regolamento sulla privacy” per informare gli utenti sull'utilizzo dei dati personali raccolti; 3. Conoscere (ed esercitare) i propri diritti in termini di privacy e sicurezza.

**Il documento, inoltre, chiarisce descrittori e livelli di padronanza e richiama anche alcune modalità valutative. A tale proposito si suggerisce l'uso delle rubriche valutative.**

## ***2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica***

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

Fondamentale, infatti, che vi sia attenzione all'uso delle TIC nella didattica poiché un loro utilizzo strutturato e integrato non solo può rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi, ma permette al docente di guidare studenti e studentesse rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento al di fuori della scuola; inoltre, questi permettono di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona. Si suggerisce, a tale proposito, di visitare il canale youtube [App Per Prof.](#)

## ***2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali***

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

Formare i docenti sulle tematiche in oggetto vuol dire non pensare esclusivamente all'alfabetizzazione ai media ma anche considerare la sfera emotiva e affettiva degli studenti e delle studentesse che usano le nuove tecnologie. Essi/e, infatti, comunicano, esprimono se stessi e sviluppano l'identità personale e sociale, attraverso i dispositivi tecnologici che sempre di più consentono loro di poter entrare in contatto con il mondo che li circonda. Prestare attenzione a questi aspetti significa dare loro gli strumenti per poter educare ragazzi e

ragazze alle emozioni in contesto onlife e quindi modulare e gestire i propri ed altrui comportamenti, favorendo e promuovendo forme di convivenza civile.

Sarebbe auspicabile pensare a momenti formativi di approfondimento (progetti specifici, laboratori, eventi, giornate, etc, ...) con la famiglia e gli/le studenti/studentesse in modo da sensibilizzare l'intera comunità educante sia su un corretto uso delle tecnologie digitali sia sulle potenzialità della Rete.

Si potrebbe anche pensare ad un cronoprogramma che consideri il triennio scolastico, in un'ottica di vera e propria programmazione, con azioni specifiche. Per esempio:

1. **Analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;**
2. **Promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse".**
3. **Monitorare le azioni svolte per mezzo di specifici momenti di valutazione;**
4. **Organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.**

Potrebbe essere predisposta un'area specifica sul sito dell'Istituto con materiali formativi per gli insegnanti. Nella sezione, potrebbero essere messi a disposizione materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet, prevedendo possibilità e modalità di condivisione fra gli insegnanti.

Sempre sul sito istituzionale della scuola, sarebbe auspicabile includere link e materiali informativi del progetto "Generazioni connesse", a partire dall'inserimento del link del progetto: [www.generazioniconnesse.it/](http://www.generazioniconnesse.it/) dove trovare ulteriori approfondimenti, spunti aggiornamenti e strumenti didattici utili da usare con gli studenti e le studentesse, per ciascun grado di scuola.

## ***2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità***

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

Il "Patto di Corresponsabilità" è un documento centrale per ogni istituzione scolastica e per la comunità educante tutta. Per questo, recentemente è stato avviato dal Miur un percorso di revisione finalizzato a definire in modo più dettagliato modalità,

tempi e ambiti della partecipazione da parte di genitori e studenti alla vita scolastica. E ciò, anche al fine di creare una maggiore collaborazione e condivisione degli interventi di formazione e di contrasto al bullismo e al cyberbullismo all'interno della comunità educante.

Per chiarire meglio il percorso di revisione del “Patto di Corresponsabilità” il MIUR ha pubblicato le [Linee di indirizzo “Partecipazione dei genitori e corresponsabilità educativa”](#). Il “Patto di Corresponsabilità educativa”, si legge, punta a “rafforzare il rapporto scuola/famiglia in quanto nasce da una comune assunzione di responsabilità e impegna entrambe le componenti a condividerne i contenuti e a rispettarne gli impegni”.

Aggiornare il “Patto di corresponsabilità” con specifici riferimenti all’uso delle tecnologie digitali e all’ePolicy è fondamentale, quindi, per informare e rendere partecipi le famiglie sul percorso che volete intraprendere con il documento e il piano d’azione.

A tale proposito è importante informare i genitori sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli.

Ad esempio, si suggerisce di:

- **elaborare regole sull’uso delle tecnologie digitali** da parte dei genitori nelle comunicazioni con la scuola e con i docenti (es. mail, gruppo whatsapp, sito della scuola etc.) e informarli adeguatamente anche riguardo alle regole per gli studenti e le studentesse;
- **fornire ai genitori consigli o linee guida sull’uso delle tecnologie digitali nella comunicazione** con i figli e in generale in famiglia (ad es. a tal fine si potrà fare riferimento alla sezione dedicata ai genitori del sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it) e fare un richiamo ad essa anche sul sito web della scuola);
- **organizzare percorsi di sensibilizzazione e formazione dei genitori** su un uso responsabile e costruttivo della Rete in famiglia e a scuola.
- **prevedere azioni e strategie per il coinvolgimento delle famiglie** in tali percorsi di sensibilizzazione, ad esempio, mediante l’organizzazione di iniziative in cui anche gli studenti e le studentesse siano protagonisti.

Una particolare attenzione potrà essere dedicata a consigli, indicazioni e informazioni su iniziative e azioni della scuola, in riferimento ai rischi connessi ad un uso distorto della Rete da parte degli studenti e delle studentesse.

Ciò in continuità anche con l’art. 5 (comma 2) della legge 29 maggio 2017, n.71 “Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo” che prevede l’integrazione, oltre che del regolamento scolastico, anche del “Patto di Corresponsabilità”, con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari “commisurate alla gravità degli atti compiuti”, al fine di meglio regolamentare l’insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

## **Il nostro piano d'azioni**

### **AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)**

#### **Scegliere almeno 1 di queste azioni**

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

### **AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi)**

#### **Scegliere almeno 1 di queste azioni**

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

# Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

---

## *3.1 - Protezione dei dati personali*

*“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. <http://www.garanteprivacy.it/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 lo scorso 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.**

Sono dati personali le 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, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati cosiddetti sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, 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 relativi a condanne penali e reati: si tratta dei dati cosiddetti giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad 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) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle tecnologie digitali, altri dati personali 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.

Le parti in gioco, quando si parla di protezione dei dati personali, sono:

- 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).

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.

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. Per tali trattamenti non sono tenute a chiedere il consenso degli/le studenti/esse.

Il liceo scientifico Nicolò Copernico ha provveduto ad aggiornare l'infrastruttura di Rete attraverso una rete Wi-fi adeguata a supportare il traffico dati generato dalle indispensabili operazioni didattiche, dalla compilazione del registro elettronico a tutte le iniziative che rientrano nelle specifiche programmazioni disciplinari che facciano ricorso all'uso delle TIC.

Ogni aula è dotata di computer, alcune anche di LIM o Digital board; è inoltre curata la dematerializzazione dei dati e la comunicazione e condivisione di informazioni tramite registro elettronico e/o Google workspace.

Agli alunni è richiesto uso corretto dei device personali, tramite circolare specificamente informativa delle regole fissate.

Il sito web istituzionale cura la sicurezza e la protezione dei dati trattati.

La e-policy fa inoltre riferimento al Regolamento di Istituto ampliato con la parte riguardante l'uso delle TIC e la protezione dei dati personali.

## ***3.2 - Accesso ad 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, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. 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.

La pianificazione che riguarda l'acquisizione, la gestione e il mantenimento dell'infrastruttura e dei device non può essere pensata se non all'interno della strategia che la scuola intende adottare attraverso l'e-Policy. È necessario, dunque, tenere in considerazione due aspetti:

- **lo status quo**, cioè la disponibilità attuale di tecnologia nella scuola e come rendere l'infrastruttura sicura, accessibile ma anche funzionante e adatta allo scopo. Per questo può essere utile avviare progetti pilota che permettano una sperimentazione e un acquisto più razionale e dilazionato degli strumenti, raccordandosi sempre con l'animatore digitale.
- **l'analisi dei bisogni della scuola** (o del plesso), in relazione alle reali esigenze didattiche e agli obiettivi prefissati. Questo permette di pianificare e di cogliere eventuali occasioni che possono presentarsi sotto forma di bandi, donazioni o finanziamenti.

Il PNSD prevede che "ogni scuola debba essere raggiunta da fibra ottica, o comunque da una connessione in banda larga o ultra-larga, sufficientemente veloce per permettere, ad esempio, l'uso di soluzioni cloud per la didattica e l'uso di contenuti di apprendimento multimediali e che le strutture interne alla scuola devono essere in grado di fornire, attraverso cablaggio LAN

o wireless, un accesso diffuso, in ogni aula, laboratorio, corridoio e spazio comune". Per questo è necessario non solo il monitoraggio di opportunità in tal senso tramite bandi PON o europei, ma anche interloquire con le amministrazioni locali. Tale adeguamento va perseguito nell'ottica di un potenziamento delle condizioni didattiche e laboratoriali necessarie a migliorare la formazione e i processi di innovazione delle istituzioni scolastiche con l'adozione di opportuni strumenti organizzativi e tecnologici.

Presso il liceo Copernico l'accesso a Internet è garantito grazie alla disponibilità di personal computer in ogni aula o ambiente scolastico. Le impostazioni sono definite e mantenute dai tecnici informatici e ogni docente deve segnalare malfunzionamenti e disservizi. I docenti accedono in autonomia ai siti web dalle postazioni a loro riservate; gli alunni accedono a Internet durante l'attività didattica su autorizzazione degli insegnanti, anche nel caso del BYOD (Bring Your Own Device).

**Dunque, gli studenti si impegnano a:**

- *utilizzare la rete nel modo corretto*
- *rispettare le consegne dei docenti*
- *non scaricare materiali e software senza autorizzazione*
- *non utilizzare unità removibili personali senza autorizzazione*
- *tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo*
- *durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste*
- *segnalare immediatamente materiali inadeguati ai propri insegnanti.*

**I docenti si impegnano a:**

- *utilizzare la rete nel modo corretto*
- *non utilizzare device personali se non per uso didattico*
- *formare gli studenti all'uso della rete*
- *dare consegne chiare e definire gli obiettivi delle attività*
- *monitorare l'uso che gli studenti fanno delle tecnologie a scuola*

Se l'accesso a Internet è un diritto, esso deve anche essere adeguato all'età degli utenti.

Per questo la scuola deve prendere tutte le necessarie precauzioni per evitare l'accesso online da parte di studenti e studentesse, a materiali non adatti a loro all'interno della scuola. Questo può avvenire attraverso l'adozione di sistemi di filtraggio software e hardware o attraverso Internet provider che forniscono un servizio ad hoc.

## Checklist per la cybersecurity

- **Mantenere separate le reti didattica e segreteria:** importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall.
- **Aggiornare periodicamente software e Sistema operativo:** garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- **Definire la programmazione di backup periodici:** cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline).
- **Garantire formazione adeguata allo staff, incluso il corpo docenti:** la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
- **Testare regolarmente le possibili vulnerabilità.**
- **Preparare piani di azione in risposta ai problemi più seri:** è importante non dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione.
- **Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo:** se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate.
- **Impostare il browser per l'eliminazione dei cookies alla chiusura:** in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione.
- **Definire una policy sulle password: le password devono essere forti:**
  - · Richiedere password complesse con almeno 8 caratteri con numeri, maiuscole e minuscole e caratteri speciali.
  - · Sensibilizzare rispetto al non uso di password facilmente identificabili (nomi dei figli, compleanni, etc.).
  - · Non memorizzare le password nei dispositivi scolastici.
  - · Non condividere le password con nessuno.
- **Minimizzare i privilegi amministrativi:** solo poche persone autorizzate dovrebbero avere privilegi amministrativi. Studenti e la maggior parte dei docenti possono accedere con account con permessi limitati.
- **Sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile):** deve riguardare chiunque abbia accesso alla Rete, studenti/esse, docenti, amministrazione e segreteria, includere i dispositivi della scuola e quelli personali, anche in caso di BYOD.

### ***3.3 - 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.

Per questo presso il Liceo scientifico Copernico sono stati tenuti negli anni diversi corsi di aggiornamento rivolti ai docenti per implementare l'uso delle tecnologie nella didattica, per approfondimenti all'interno della programmazione e per rendere efficiente l'uso di Google non solo nella DAD (workspace, Classroom, Meet, Jamboard). L'uso dei dispositivi personali (BYOD) è normato da regolamento e previsto solo in accordo con i docenti.

Quando ci si relaziona attraverso l'uso di strumenti di comunicazione online, si mette in atto una modalità comunicativa che ha caratteristiche e logiche proprie. Ecco, allora, alcuni aspetti importanti da tenere in considerazione e di cui è importante essere consapevoli quando si fa uso delle TIC nelle comunicazioni a scuola: non si condividono lo stesso spazio e lo stesso contesto comunicativo con gli interlocutori; per questo, talvolta, può accadere che si forniscano cornici interpretative molto diverse ai messaggi e ai contenuti scambiati. La comunicazione online, inoltre, generalmente non permette di accedere ai cosiddetti segnali della comunicazione non verbale (tono della voce, espressione del volto, gesti del corpo, pause...etc.) e non si è in grado di vedere ed ascoltare direttamente gli effetti della propria comunicazione sull'interlocutore. Il cosiddetto feed-back non tangibile e l'impossibilità di accedere ai segnali non verbali dell'interlocutore, così come la distanza e la separazione mediante lo schermo, rendono meno empatici e quindi meno attenti a emozioni e potenziali reazioni dell'altra persona. Inoltre, la comunicazione che viaggia online, generalmente, si avvale di messaggi scritti che possono essere memorizzati, diffusi e permangono nel tempo. È sempre bene tenerlo a mente. Così come è invece utile apprendere modalità che consentono di usare un linguaggio multimediale, ipertestuale e accattivante, tale da promuovere la partecipazione e il coinvolgimento dei diversi attori.

Quali strumenti di comunicazione online possono essere utilizzati a scuola?

A tale proposito è importante effettuare una distinzione preliminare fra comunicazione esterna e comunicazione interna. La prima consente di trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che l'Istituto porta avanti e comporta la condivisione di regole ben precise su cosa comunicare e come comunicarlo. Fra gli strumenti di comunicazione interna, invece, troviamo principalmente il registro elettronico con tutte le sue funzionalità, o ulteriori applicativi e piattaforme di lavoro condiviso e collaborativo come [wiki](#), [google doc](#), [classroom](#) che possono essere ampiamente utilizzati anche per facilitare e rendere più partecipata la didattica e la comunicazione a scuola.

### ***3.4 - 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.

La presente *ePolicy* contiene 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 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.

Di seguito, i dieci punti del Miur per l'uso dei dispositivi mobili a scuola, BYOD (Bring your own device):

1. **Ogni novità comporta cambiamenti.** Ogni cambiamento deve servire per migliorare l'apprendimento e il benessere delle studentesse e degli studenti e più in generale dell'intera comunità scolastica
2. **I cambiamenti non vanno rifiutati, ma compresi e utilizzati per il raggiungimento dei propri scopi.** Bisogna insegnare a usare bene e integrare nella didattica quotidiana i dispositivi, anche attraverso una loro regolamentazione. Proibire l'uso dei dispositivi a scuola non è la soluzione. A questo proposito ogni scuola adotta una Politica di Uso Accettabile (PUA) delle tecnologie digitali.
3. **La scuola promuove le condizioni strutturali per l'uso delle tecnologie digitali.** Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile dei dispositivi personali (BYOD). Le tecnologie digitali sono uno dei modi per sostenere il rinnovamento della scuola.

4. **La scuola accoglie e promuove lo sviluppo del digitale nella didattica.** La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica. Dirigenti e insegnanti attivi in questi campi sono il motore dell'innovazione. Occorre coinvolgere l'intera comunità scolastica anche attraverso la formazione e lo sviluppo professionale.
5. **I dispositivi devono essere un mezzo, non un fine.** È la didattica che guida l'uso competente e responsabile dei dispositivi. Non basta sviluppare le abilità tecniche, ma occorre sostenere lo sviluppo di una capacità critica e creativa.
6. **L'uso dei dispositivi promuove l'autonomia delle studentesse e degli studenti.** È in atto una graduale transizione verso situazioni di apprendimento che valorizzano lo spirito d'iniziativa e la responsabilità di studentesse e gli studenti. Bisogna sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione, anche in vista di un apprendimento lungo tutto l'arco della vita.
7. **Il digitale nella didattica è una scelta: sta ai docenti introdurla e condurla in classe.** L'uso dei dispositivi in aula, siano essi analogici o digitali, è promosso dai docenti, nei modi e nei tempi che ritengono più opportuni.
8. **Il digitale trasforma gli ambienti di apprendimento.** Le possibilità di apprendere sono ampliate, sia per la frequentazione di ambienti digitali e condivisi, sia per l'accesso alle informazioni, e grazie alla connessione continua con la classe. Occorre regolamentare le modalità e i tempi dell'uso e del non uso, anche per imparare a riconoscere e a mantenere separate le dimensioni del privato e del pubblico.
9. **Rafforzare la comunità scolastica e l'alleanza educativa con le famiglie.** È necessario che l'alleanza educativa tra scuola e famiglia si estenda alle questioni relative all'uso dei dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione. Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.
10. **Educare alla cittadinanza digitale è un dovere per la scuola.** Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

## *Il nostro piano d'azioni*

**AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).**

**Scegliere almeno 1 di queste azioni:**

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto

per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola

- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

#### **AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).**

##### **Scegliere almeno 1 di queste azioni:**

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.

- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

# Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

---

## *4.1 - Sensibilizzazione e Prevenzione*

**Il rischio online si configura come la possibilità per il minore di:**

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non

piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione**.

Nel caso della **sensibilizzazione** si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.

Nel caso della **prevenzione** si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

La comunità scientifica internazionale utilizza la classificazione proposta dall'Institute of Medicine che distingue tre livelli di prevenzione:

**Prevenzione Universale.** Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale. Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che "trattano" un gruppo con un problema specifico.

Tuttavia, questi interventi possono produrre cambiamenti in grandi

popolazioni (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale).

**Prevenzione Selettiva.** Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti.

**Prevenzione Indicata.** Un programma di intervento sul caso specifico, è quindi pensato e strutturato per adattarsi agli/le studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/la ragazzo/a.

Il liceo Copernico ha curato, negli anni, la prevenzione di primo livello, a carattere universale, ospitando relatori che tenessero conferenze sul tema o partecipando a progetti che prevedessero relazioni e conseguenti discussioni sul tema; ed ha pure percorso la strada della sensibilizzazione iscrivendo classi di alunni a concorsi di vario genere che li portassero a riflettere sia sulle dinamiche psicologiche di

comportamenti errati, legati a situazioni di rischio online, sia sulle caratteristiche rappresentative dei fenomeni del cyberbullismo; gli alunni hanno potuto esprimersi adottando linguaggi diversi, figurativo o verbale, e hanno appreso meccanismi di motivazione al cambiamento o hanno indicato soluzioni fondate sulla consapevolezza dei problemi.

L'informazione dovrà comunque sempre riguardare: uso e abuso di internet; dipendenza dai dispositivi elettronici; consapevolezza dei pericoli della rete; conoscenza dell'importanza di tutelare la propria privacy e quella degli altri e delle implicazioni legali in caso di trasgressione; conoscenza delle regole e norme etiche sulla navigazione in rete e sulla condivisione di contenuti; conoscenza della normativa del settore e delle conseguenze penali in caso di violazione.

## ***4.2 - Cyberbullismo: che cos'è e come prevenirlo***

La legge 71/2017 “Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo”, nell'art. 1, comma 2, definisce il cyberbullismo:

*“qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per*

*via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo”.*

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
  - promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
  - previsione di misure di sostegno e rieducazione dei minori coinvolti;
  - Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte [di cyberbullismo](#) e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;

Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie:

**Nomina del Referente per le iniziative di prevenzione e contrasto che:**

Ha il compito di coordinare le iniziative di prevenzione e contrasto del [cyberbullismo](#). A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

5

Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Tratti specifici del bullismo online sono correlati all'impatto che le tecnologie digitali hanno nella vita dei ragazzi (e di tutti) e alle caratteristiche stesse della Rete: la convinzione dell'anonimato, l'assenza di confini spaziali, l'assenza di limiti temporali, l'indebolimento dell'empatia, il feedback non tangibile, la percezione che online non ci siano norme sociali, la sperimentazione online di identità multiple, il contesto virtuale come luogo di simulazione, la diffusione di responsabilità.

Il liceo Copernico ha aderito alle attività previste da una rete di scopo, includendo nella prevenzione all'interno dell'Istituto una scheda di segnalazione di eventuali atti di bullismo e la preparazione di alcuni alunni formati ad agire in un processo di peer education; può poi usufruire del protocollo di intervento approntato dalla stessa rete di scopo, in collaborazione sia con le forze dell'ordine sia con associazioni presenti sul territorio che si occupano di percorsi di rieducazione/riabilitazione.

### ***4.3 - Hate speech: che cos'è e come prevenirlo***

Il fenomeno di “incitamento all’odio” o “discorso d’odio”, indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine “hate speech” indica un’offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

**Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l’obiettivo di:**

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all’orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l’impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Il liceo Copernico, favorendo l'espressione anche multimediale degli alunni e preparandola con un'educazione etica che attinge ai vari contenuti disciplinari in correlazione con l'educazione civica trasversale, interviene per promuovere riconoscimento e prevenzione dei discorsi d'odio rendendo consapevoli che:

- il discorso d'odio procura sofferenza
- gli atteggiamenti alimentano gli atti
- l'odio online non è solo espresso a parole
- l'odio prende di mira sia gli individui sia i gruppi
- internet è difficilmente controllabile
- l'odio ha radici profonde
- l'odio si avvantaggia con la creduta impunità e il presunto anonimato
- l'espressione di odio riguarda contenuto, tono e intenzione, il contesto e i bersagli potenziali
- occorre apprendere un uso consapevole delle tecnologie
- occorre decostruire gli stereotipi
- occorre costruire l'attitudine alla partecipazione civica e all'impegno.

## ***4.4 - Dipendenza da Internet e gioco online***

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza,

problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

*L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale*

E' necessario prendere atto che caratteristiche della dipendenza da Internet (Internet Addiction Disorder) sono:

- dominanza, alterazioni del tono dell'umore, conflitto, ricaduta, alterazioni della percezione del tempo, astinenza che subentra alla tolleranza, ansia e nomofobia (no-mobile), agitazione psicomotoria, fantasie, pensieri ossessivi, ripercussioni sulla sfera delle relazioni interpersonali cui si preferisce il mondo virtuale.

Viceversa, il benessere digitale, che può essere insegnato tramite l'esempio correttamente dato nel momento dell'integrazione delle tecnologie nella didattica, dipende da:

- ricerca di equilibrio anche nelle relazioni online, uso di strumenti digitali per il raggiungimento di obiettivi personali, capacità di interagire negli ambiti digitali in modo sicuro e responsabile, capacità di gestire il sovraccarico informativo e le distrazioni (per esempi, le notifiche).

## ***4.5 - Sexting***

Il “sexting” è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti medialmente sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

L'Istituto è attento all'ascolto degli studenti riguardo allo scambio di contenuti multimediali non appropriati, anche attraverso lo Sportello di ascolto psicologico.

Tra le caratteristiche del fenomeno vi sono principalmente:

- **la fiducia tradita:** chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);
- **la pervasività con cui si diffondono i contenuti:** in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;
- **la persistenza del fenomeno:** il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

## ***4.6 - Adescamento online***

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti

utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di *teen dating* (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

**In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).**

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

L'Istituto si propone di educare gli studenti ad un comportamento critico e responsabile durante l'attività online e individua figure adulte alle quali chiedere confronto e aiuto per gestire in modo opportuno eventuali problematiche insorte con l'uso di Internet.

**Il processo di adescamento segue generalmente 5 fasi:**

1. **Fase dell'amicizia iniziale:** Questa è la fase in cui l'adescatore cerca i primi contatti con la vittima individuata, provando a socializzare con lei. Tenterà, quindi, di conoscerla meglio al fine di scoprirne bisogni, interessi e il contesto in cui vive. Condividendo argomenti di interesse del minore l'adescatore cercherà pian piano di conquistarsi la sua fiducia, ponendogli domande frequenti che attestano interesse e attenzione nei suoi confronti. Gradualmente affronterà con la vittima argomenti sempre più privati ed intimi.
2. **La fase di risk-assessment:** in seguito ai primi contatti con il minore, l'adescatore cerca di comprendere il contesto in cui si svolge l'interazione (es. da dove si collega alla Rete? I genitori lo controllano quando chatta? Che rapporto ha con loro?). L'obiettivo dell'adescatore è quello di rendere sempre più privato ed "esclusivo" il rapporto, cercando di passare, ad esempio, da una chat pubblica ad una privata, da una chat alle conversazioni attraverso il telefono, per poterne così carpire il numero.
3. **Fase della costruzione del rapporto di fiducia:** le confidenze e le tematiche affrontate divengono via via più private ed intime o comunque molto personali. In questa fase l'adescatore può iniziare a fare regali di vario tipo alla vittima e può anche avvenire lo scambio di foto, subito e non necessariamente a sfondo sessuale.
4. **Fase dell'esclusività:** l'adescatore rende la relazione con il minore sempre più "segreta", isolandolo sempre più dalla famiglia e dagli amici. Chiederà alla vittima di non raccontare a nessuno ciò che sta vivendo. L'esperienza reciproca verrà presentata come un "geloso segreto" da custodire per non rovinare tutto. In questa fase l'adescatore potrà ricorrere a ricatti morali puntando sulla fiducia costruita, sulla paura o sul senso di colpa.
5. **Fase della relazione sessualizzata:** in questa fase la richiesta di immagini o video sempre più privati e a sfondo erotico potrebbe essere più insistente, così come la proposta di incontri offline. Qualora il minore avesse già inviato immagini o video privati, potrebbe essere ricattato dall'adescatore: se non accettasse un eventuale incontro l'adescatore potrebbe diffondere quel materiale online. Questi, inoltre, tenderà a presentare sempre la situazione come "normale" al fine di vincere le eventuali resistenze del minore a coinvolgersi in tale rapporto.

E' possibile avvalersi, nel riconoscere il rischio di avvenuto adescamento, dei seguenti segnali:

- Il minore ha conoscenze sessuali non adeguate alla sua età?
- Si viene a conoscenza di un certo video o di una foto che circola online o che il minore ha ricevuto o filmato, ma c'è imbarazzo e preoccupazione nel raccontare di più.

- Il minore si isola totalmente e sembra preso solo da una relazione online?
- Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove.

Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video...).

L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi, ma anche di provare un senso di colpa per essere caduti in trappola ed essersi fidati di uno sconosciuto.

## ***4.7 - Pedopornografia***

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi

rappresentazione degli organi sessuali a fini soprattutto sessuali.

**La legge n. 269 del 3 agosto 1998** *“Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù”*, introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella **legge n. 38 del 6 febbraio 2006** *“Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet”*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest’ultima, introduce, tra le altre cose, il reato di *“pornografia minorile virtuale”* (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

**Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.)** *per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.*

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito [www.generazioniconnesse.it](http://www.generazioniconnesse.it) alla sezione “**Segnala contenuti illegali**” ([Hotline](#)).

**Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il “Clicca e Segnala” di [Telefono Azzurro](#) e “STOP-IT” di [Save the Children](#).**

L'Istituto, tramite lo Sportello di ascolto psicologico, è attento ad accogliere e a segnalare alle autorità competenti eventuali problematiche, qualora dovessero emergere. Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità.

## **Il nostro piano d'azioni**

**AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).**

**Scegliere almeno 1 di queste azioni:**

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/le studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale

della scuola.

- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

**AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).**

**Scegliere almeno 1 di queste azioni:**

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle

studenti/studentesse.

- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

# Capitolo 5 - Segnalazione e gestione dei casi

---

## 5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

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. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso**.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

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.**

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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 la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via 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.

Al fine di contrastare le infrazioni alla E-policy di Istituto, la scuola si impegnerà a gestire i casi, previa raccolta delle segnalazioni; sono utili la Scheda di segnalazione e il Diario di bordo, con schema riepilogativo delle situazioni gestite. **Si allega il protocollo per l'intervento del Team operativo della rete di scopo "Nessuno si salva da solo".**

## ***5.2. - Come segnalare: quali strumenti e a chi***

L'insegnante riveste la qualifica di pubblico ufficiale 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.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.....

Come descritto nelle procedure di questa sezione, si potrebbero palesare due 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.

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.

Per tutti i dettagli si fa riferimento 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.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:19696).

Se non si ravvisano fattispecie di reato, si dovrebbe:

- informare i genitori (o chi esercita la responsabilità genitoriale) degli/delle studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo, su quanto accade e condividere informazioni e strategie;
- richiedere, in concomitanza, la consulenza dello psicologo scolastico a supporto della gestione della situazione, in base alla gravità dell'accaduto;
- informare i genitori degli/delle studenti/studentesse infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy);
- informare gli/le studenti/studentesse ultra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy);
  - attivare il consiglio di classe;
  - valutare come coinvolgere gli operatori scolastici su quello che sta accadendo.

A seconda della situazione e delle valutazioni effettuate con referente, dirigente e genitori, si potrebbe poi segnalare alla Polizia Postale: a) contenuto del materiale online offensivo; b) modalità di diffusione; c) fattispecie di reato eventuale.

### ***5.3. - Gli attori sul territorio***

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

**Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.

**Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.

**Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.

**Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.

**Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

**Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnalano all'Autorità giudiziaria e ai Servizi sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovuti a situazioni ambientali carenti o inadeguate.

**Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

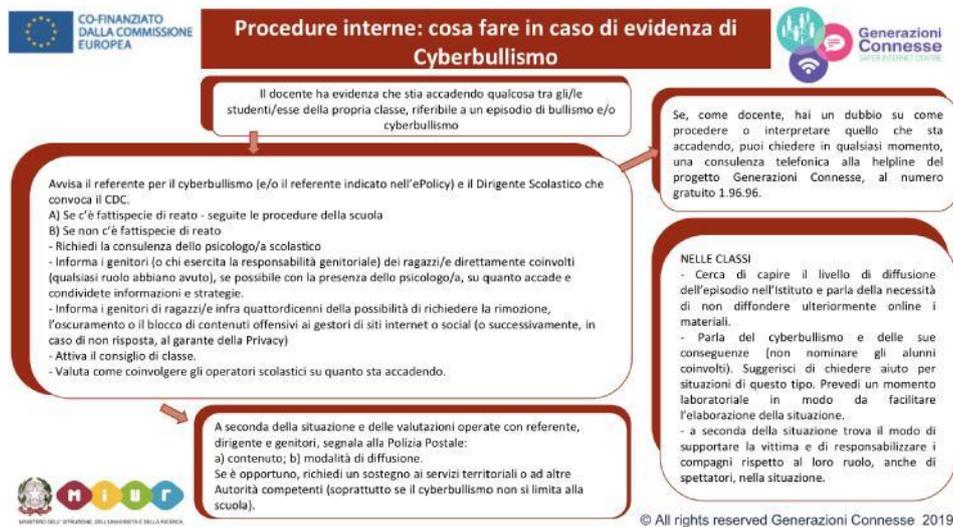
L'Istituto provvede a mantenere rapporti costanti con le Associazioni presenti sul territorio che si occupano di sensibilizzare su tali tematiche.

L'Ufficio scolastico regionale supporta l'Istituto nella diffusione di iniziative volte alla prevenzione dei fenomeni.

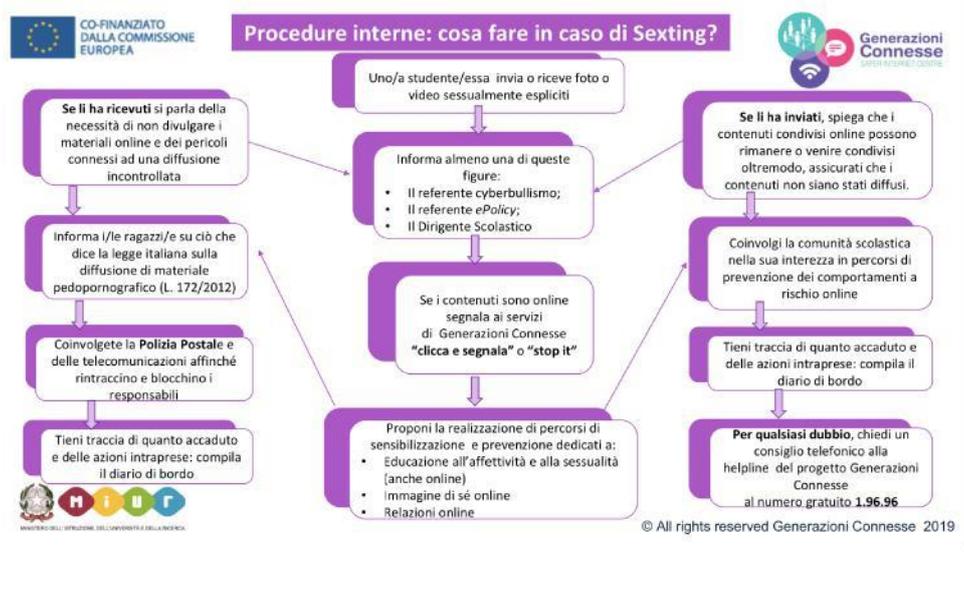
Nell'ambito del protocollo previsto dalla rete di scopo è inoltre stabilito un raccordo con le autorità preposte alla segnalazione e al trattamento di eventuali casi riscontrati.

## 5.4. - Allegati con le procedure

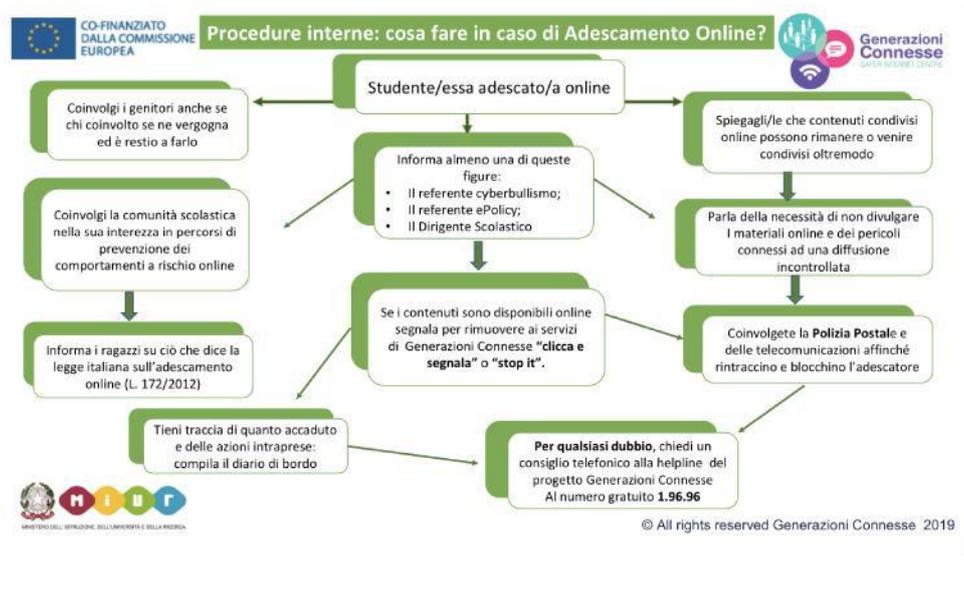
### Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



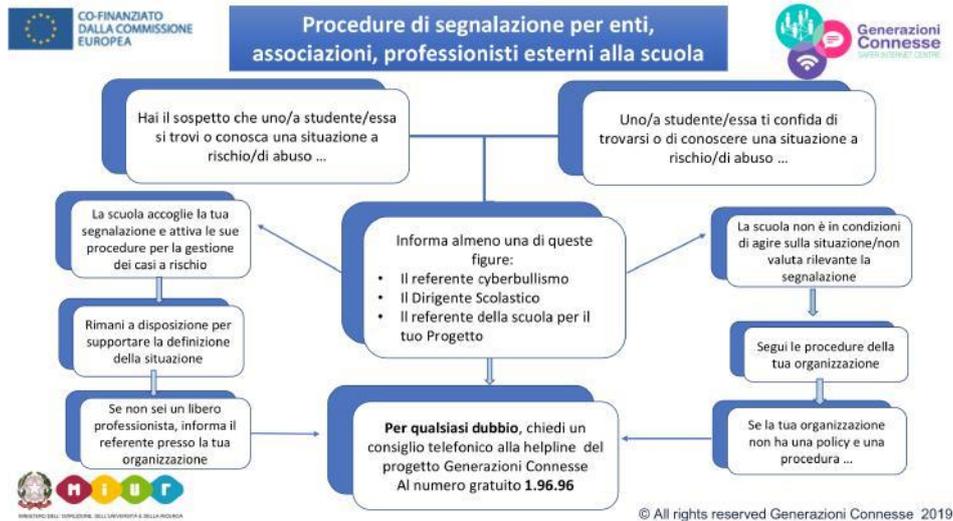
### Procedure interne: cosa fare in caso di sexting?



## Procedure interne: cosa fare in caso di adescamento online?



## Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



## Altri allegati

- [Scheda di segnalazione](#)
- [Diario di bordo](#)
- [iGloss@ 1.0 l'ABC dei comportamenti devianti online](#)
- [Elenco reati procedibili d'ufficio](#)

## *Il nostro piano d'azioni*

La referente per la prevenzione del Cyberbullismo  
Prof.ssa Maria Braschi

