



## Documento di ePolicy

ISTITUTO DI ISTRUZIONE SUPERIORE  
ENRICO MATTEI - MITD52000  
VIA PADRE VAIANI 18  
20017 - RHO (MI)

## **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 visione educativa e la proposta formativa dell'Istituto, in riferimento alle tecnologie digitali. Nello specifico:

- 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 formativo ed educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni a rischio 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 curricolo

1. Curricolo 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 alle nuove tecnologie. L' E-policy fornisce 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 sulle tecnologie digitali.

L'ePolicy è un documento programmatico volto a promuovere le competenze digitali ed un uso positivo, critico e consapevole delle nuove tecnologie, sia da parte degli studenti che da parte del personale scolastico.

Nello specifico, è un documento programmatico autoprodotta dalla scuola volto a descrivere:

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

Tra i principi che l'Istituto Mattei riconosce e garantisce, vi sono il rispetto reciproco e la condivisione delle regole scolastiche, il diritto alla riservatezza, la trasparenza dell'attività amministrativa.

In merito al rispetto reciproco e alla condivisione delle regole scolastiche, tutte le componenti che operano all'interno dell'Istituto (studenti, docenti, Dirigente scolastico e collaboratori, personale amministrativo, genitori) si impegnano a collaborare in maniera costruttiva nell'assolvere le rispettive funzioni, scongiurando e condannando atteggiamenti arroganti, intimidatori, prevaricatori o violenti, soprattutto quelli a danno dei soggetti socialmente più deboli e svantaggiati. Per tale ragione tutte le componenti scolastiche si impegnano a conoscere e a rispettare, oltre che la normativa vigente, anche il Piano triennale dell'offerta formativa (PTOF), il Regolamento di Istituto (in particolare le sezioni relative al Regolamento di disciplina e al Regolamento sul bullismo e il cyberbullismo), il Patto di corresponsabilità scuola- famiglie e il presente documento di ePolicy.

In riferimento alla riservatezza, Dirigente scolastico e collaboratori, docenti e personale amministrativo, si impegnano a non divulgare dati personali e notizie riservate di cui vengono a conoscenza nell'esercizio delle loro funzioni. Gli studenti si impegnano a rispettare il diritto alla riservatezza dei propri compagni e degli operatori scolastici non diffondendo in alcun modo informazioni riservate, immagini, audio, video ecc. senza il consenso dei diretti interessati (a tale proposito si veda la Sezione "Uso dei cellulari e di altri dispositivi elettronici" del Regolamento di Istituto).

L'Istituto Mattei, inoltre, si conforma ai principi della trasparenza, imparzialità e buon andamento dell'azione amministrativa. Si impegna pertanto ad agevolare gli interessati all'accesso alle informazioni e a comunicarle in modo tempestivo anche tramite il Registro elettronico. Si sottolinea che gli studenti hanno diritto alla trasparenza del processo valutativo, ossia di conoscere in modo chiaro e tempestivo le modalità e i criteri di valutazione.

Le modalità di comunicazione con docenti, studenti e genitori comprendono il Registro elettronico, il Sito web della scuola, la posta elettronica ordinaria ed, eventualmente, la posta elettronica certificata (PEC). Il personale in servizio può comunicare via chat, e-mail, telefono o social media ecc. con gli studenti esclusivamente per svolgere od organizzare attività di natura puramente didattica. E' fatto assoluto divieto di pubblicare audio, video, immagini senza il previo consenso dei soggetti interessati. Chiunque venga a conoscenza di attività espressamente vietate dalla legge o dal Regolamento d'Istituto è tenuto a darne comunicazione al Dirigente scolastico.

---

## 1.2 - Ruoli e responsabilità

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

## **Il Dirigente Scolastico**

Il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. Segue corsi di formazione e di aggiornamento sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del Ministero dell'istruzione; promuove la cultura della sicurezza online e fornisce il proprio contributo all'organizzazione, insieme ai docenti referenti per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Presiede il Team per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo. Interviene nei casi bullismo, cyberbullismo ed uso improprio delle tecnologie digitali. Gestisce in prima persona, in collaborazione con i referenti e i docenti dei Consigli di classe, i casi gravi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

In merito alle attività di formazione sull'uso corretto delle nuove tecnologie e di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo, il Dirigente scolastico:

- definisce 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 bullismo e del cyberbullismo; favorisce l'adozione e l'aggiornamento di regole condivise inserite nel Regolamento di Istituto e di disciplina per il contrasto e la prevenzione dei fenomeni di bullismo e cyberbullismo;
- previene e contrasta fenomeni di bullismo e cyberbullismo nel rispetto della normativa vigente;
- assicura 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 [www.generazioniconnesse.it](http://www.generazioniconnesse.it) per tutte le altre informazioni di carattere generale;
- promuove, diffonde e coordina azioni educative e corsi di aggiornamento finalizzati a sensibilizzare l'intera comunità scolastica (studenti, genitori, personale non docente e docente) in materia di bullismo e cyberbullismo, a livello territoriale, anche in rete con enti, associazioni, istituzioni locali e altre scuole, coinvolgendo esperti;
- garantisce l'utilizzo sicuro di Internet a scuola, promuovendo la conoscenza sia dei contenuti tecnologici, sia delle implicazioni psicopedagogiche correlate;
- attiva 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 agli studenti coinvolti;
- nomina uno o più referenti per la prevenzione e il contrasto del bullismo e cyberbullismo, individuati dal Collegio dei Docenti.

## **L'Animatore digitale**

L'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online e alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale"; monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per

scopi istituzionali e consentiti (istruzione e formazione).

In merito alle attività di formazione sull'uso corretto delle nuove tecnologie e di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo, l'Animatore digitale promuove attività formative destinate agli studenti e al personale scolastico e interviene, su richiesta del Dirigente scolastico, nelle attività di prevenzione e di contrasto dei fenomeni di bullismo e di cyberbullismo.

L'Animatore digitale partecipa alla Commissione per la Transizione ecologica e digitale e al Team per l'innovazione, promuovendo all'interno dell'Istituto attività formative e di aggiornamento.

### **I Referenti per la prevenzione e il contrasto del bullismo e del cyberbullismo**

Secondo quanto disposto dall'art. 4 della Legge n. 71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo", all'interno del personale docente dell'Istituto Mattei, sono stati individuati due referenti con il compito di coordinare le iniziative di prevenzione e di contrasto del bullismo e del cyberbullismo.

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 può coinvolgere, con progetti e percorsi formativi ad hoc, studenti, docenti e genitori.

In merito alle attività di formazione sull'uso corretto delle nuove tecnologie e di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo, il Referente bullismo e cyberbullismo:

- costituisce 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;
- promuove azioni educative, iniziative e corsi di aggiornamento in materia di bullismo e del cyberbullismo attraverso progetti d'Istituto che coinvolgano genitori, studenti e tutto il personale;
- coordina le attività di formazione sull'utilizzo corretto delle nuove tecnologie e, in particolare, sulle responsabilità di natura civile e penale, anche avvalendosi della collaborazione delle Forze di polizia, nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio;
- si coordina con esperti esterni alla scuola (associazioni, servizi sociali e sanitari, aziende, forze dell'ordine, ecc.) per realizzare progetti di prevenzione;
- cura rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet ("Safer Internet Day");
- svolge un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'Istituto), atti e documenti (PTOF, PdM, Rav);
- raccoglie e diffonde le buone pratiche educative, organizzative e azioni di monitoraggio, favorendo l'elaborazione di un modello di ePolicy d'Istituto;
- partecipa a corsi di formazione, anche e tramite specifiche piattaforme sviluppate dal Ministero dell'istruzione per i docenti referenti.

## **I docenti**

I docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Per quanto possibile, integrano le tematiche specifiche della propria disciplina con approfondimenti ad hoc, promuovendo anche l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete; si impegnano a segnalare al Dirigente Scolastico qualunque problematica, violazione e abuso, anche online, che vedano coinvolti studenti e studentesse.

In merito alle attività di formazione sull'uso corretto delle nuove tecnologie e di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo, il personale docente:

- si impegna ad utilizzare correttamente i dispositivi digitali e a promuovere un utilizzo corretto delle nuove tecnologie da parte degli studenti;
- adotta le azioni e attua le iniziative deliberate dal Consiglio di Classe e dal Collegio Docenti;
- opera nel rispetto del Regolamento di Istituto e si impegna a prevenire e reprimere fenomeni di bullismo e cyberbullismo;
- diffonde la conoscenza della netiquette in rete e della normativa sulla privacy;
- segnala al Coordinatore di classe i comportamenti scorretti e i casi di bullismo e cyberbullismo di cui viene a conoscenza, direttamente o indirettamente, al fine di coinvolgere gli organi scolastici competenti (Referente del bullismo e del cyberbullismo, Consiglio di Classe o di Istituto, Dirigente scolastico);
- partecipa a corsi di formazione.

## **Il personale Amministrativo, Tecnico e Ausiliario (ATA)**

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. Il personale ATA è costituito da diverse figure che, in sinergia, si occupano, ciascuna per la propria funzione, del funzionamento dell'Istituto scolastico, che passa anche attraverso lo sviluppo della cultura digitale. E' previsto un coinvolgimento diretto 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 partecipa alla prevenzione e alla segnalazione dei comportamenti scorretti e dei casi di bullismo e cyberbullismo, insieme alle altre figure.

In merito alle attività di formazione sull'uso corretto delle nuove tecnologie e di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo, il personale ATA:

- collabora nell'attuazione delle azioni e delle iniziative deliberate dal Consiglio di Classe e dal Collegio Docenti;
- opera nel rispetto del Regolamento di Istituto, e si impegna a prevenire e reprimere fenomeni di bullismo e cyberbullismo;
- segnala al Dirigente scolastico o al Coordinatore di classe i comportamenti devianti e gli eventuali fenomeni di bullismo o cyberbullismo di cui viene a conoscenza direttamente o

indirettamente al fine di coinvolgere gli organi scolastici competenti (Referente al bullismo e al cyberbullismo, Consiglio di Classe o di Istituto);

- partecipa a corsi di formazione.

## **Gli studenti**

Gli studenti, in relazione al grado di maturità e consapevolezza raggiunta, devono utilizzare al meglio le tecnologie digitali, in coerenza con quanto previsto dal Regolamento d'Istituto e con quanto richiesto dai docenti; con il supporto della scuola, imparano a tutelarsi online e a rispettare gli altri; partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e si fanno promotori di quanto appreso, anche attraverso possibili percorsi di peer education.

Inoltre gli studenti:

- partecipano attivamente e in maniera costruttiva alle iniziative formative in materia di bullismo e cyberbullismo;
- rispettano le regole stabilite dal Regolamento di Istituto in materia di bullismo e cyberbullismo;
- segnalano al coordinatore di classe o alla Presidenza i comportamenti devianti e gli eventuali reati che coinvolgano i propri compagni di classe o altri studenti dell'Istituto, sia come vittime che come autori di atti di bullismo o cyberbullismo, di cui vengono a conoscenza, direttamente o indirettamente, al fine di coinvolgere gli organi scolastici competenti (Referente del bullismo e del cyberbullismo, Dirigente scolastico, Consiglio di Classe o di Istituto);
- i rappresentanti degli studenti, eletti negli organi collegiali d'Istituto o nella Consulta provinciale, promuovono iniziative che favoriscano la collaborazione e la prevenzione dei fenomeni di bullismo e cyberbullismo.

## **I genitori**

I genitori partecipano attivamente alle attività di formazione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicano con loro circa i problemi rilevati. Accettano e condividono quanto previsto nell'ePolicy dell'Istituto. Esiste una corresponsabilità educativa e formativa che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse. In particolare, il secondo comma dell'art. 2048 c.c. così recita: "I precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi e apprendisti nel tempo in cui sono sotto la loro vigilanza". Per i genitori, invece, bisogna considerare le seguenti norme:

- il primo comma dell'art. 30 della Costituzione "è dovere e diritto dei genitori mantenere, istruire ed educare i figli, anche se nati fuori del matrimonio";
- il primo comma dell'art. 2048 c.c. ai sensi del quale "il padre e la madre o il tutore sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone soggette alla tutela, che abitano con essi (...)";
- l'art. 147 del c.c. prevede "l'obbligo di mantenere, istruire, educare e assistere moralmente i figli, nel rispetto delle loro

capacità, inclinazioni naturali e aspirazioni (...)"

I genitori, inoltre:

- si impegnano a partecipare attivamente alle azioni di formazione/informazione, promosse dall'Istituto aventi a oggetto il bullismo e il cyberbullismo;
- vigilano sui comportamenti dei propri figli, in particolar modo sull'uso delle tecnologie digitali;
- si impegnano a prendere conoscenza delle azioni messe in campo dalla scuola e collaborano secondo le modalità previste dal Patto di corresponsabilità;
- prendono conoscenza della sezione disciplinare e della sezione bullismo e cyberbullismo del Regolamento di Istituto;
- segnalano al Coordinatore di classe o al Dirigente scolastico i comportamenti scorretti e gli eventuali reati che coinvolgano i propri figli o altri studenti dell'Istituto, sia come vittime, sia come autori, di cui vengono a conoscenza, direttamente o indirettamente.

### **Gli Enti educativi esterni e le associazioni**

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola si conformano alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; promuovono comportamenti corretti e la sicurezza online; assicurano la riservatezza dei dati personali degli studenti e delle studentesse (sul tema consultare il punto successivo).

---

### **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 dello studente, ascoltare e prendere in seria considerazione le opinioni ed i desideri degli alunni, 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 a partecipare a comportamenti di minori che siano illegali, 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 dispositivi personali (smartphone, tablet, pc, ecc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto nel corso delle attività organizzate con gli studenti. 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).

Al fine di rendere l'ePolicy uno strumento efficace per la tutela degli studenti e delle studentesse, si individua un insieme di regole o norme di comportamento da condividere con le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve e/o lungo periodo. Dotarsi di un'informativa sull'ePolicy comprensiva delle procedure di segnalazione da

condividere con tutte le figure che operano con gli studenti, significa non solo tutelare questi ultimi e la scuola stessa, ma anche porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali.

Le organizzazioni/associazioni extrascolastiche e gli esperti esterni sono tenuti a rilevare e a segnalare al Dirigente scolastico e ai Referenti bullismo e cyberbullismo le problematiche connesse ad un uso non corretto delle tecnologie digitali. In questo modo, si facilita l'intervento della scuola in chiave di prevenzione e di contrasto dei comportamenti scorretti e illeciti connessi all'utilizzo delle nuove tecnologie.

In coerenza con il percorso intrapreso e con le azioni che l'Istituto già pone in essere, la predisposizione di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione garantisce un migliore rapporto fiduciario fra scuola e famiglia, consente di distinguere i ruoli e le azioni da compiere e di attivare direttamente, a seconda della tipologia dei casi da segnalare, le autorità competenti, collaborando con i servizi del territorio per la prevenzione e la gestione di quanto rilevato, in un'ottica di gestione condivisa degli interventi.

Tutti i soggetti esterni che erogano attività in ambito scolastico sono informati sui rischi online che possono correre gli studenti e le studentesse e sui comportamenti corretti che devono adottare a scuola.

I soggetti esterni sono tenuti a segnalare qualsiasi comportamento scorretto ai docenti responsabili del progetto, al Dirigente scolastico e ai Referenti bullismo e cyberbullismo, in qualsiasi forma, comunicando, per quanto possibile, i soggetti responsabili, le eventuali vittime, una descrizione il più possibile circostanziata dell'episodio. Per questo, i soggetti esterni possono compilare la scheda di segnalazione allegata alla fine del documento di ePolicy.

La presente informativa è condivisa con il personale e le associazioni esterne: le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività ne prendono visione e si impegnano a rispettarla preliminarmente all'avvio dei programmi con gli studenti, in classe o fuori. E' a discrezione dell'Istituto richiedere agli attori esterni, eventualmente, il casellario giudiziale come fattore ulteriormente protettivo verso i minori. L'obiettivo è quello di verificare l'esistenza (o meno) di condanne per alcuni reati previsti dal Codice penale e nello specifico gli articoli 600-bis (prostituzione minorile), 600-ter (pornografia minorile), 600-quater (detenzione di materiale pornografico), 600-quinquies (iniziative turistiche volte allo sfruttamento della prostituzione minorile), 609-undecies (adescamento di minorenni), o l'irrogazione di sanzioni interdittive all'esercizio di attività che comportino contatti diretti e regolari con i minori. L'eventuale presenza di un codice di condotta adottato dalla propria organizzazione o associazione (cooperativa, ente di formazione, servizio, etc.) è un fattore preferenziale.

---

#### **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 pubblicato sul sito istituzionale 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 documento di ePolicy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. Nello specifico è importante tener presente che:

- condividere e comunicare il documento agli studenti e alle studentesse significa dare loro una base di partenza per un uso consapevole e corretto dei dispositivi e della tecnologia informatica;
- dare loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici;
- dare loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.
- è importante condividere e comunicare il documento al personale scolastico in modo da poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispositivi e della Rete, in linea anche con il Codice di comportamento dei pubblici dipendenti;
- è fondamentale condividere con i genitori il documento e pubblicarlo sul sito istituzionale della scuola. La condivisione può avvenire anche tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.

E' necessario, inoltre, che ciascun attore scolastico (dai docenti agli studenti) si faccia a sua volta promotore del documento. Ogni Consiglio di classe si occupa di informare gli studenti della classe e di verificare che si adottino comportamenti corretti nell'utilizzo delle nuove tecnologie.

Tutti gli atti fondamentali dell'Istituto (Carta dei servizi, Regolamento d'Istituto, con particolare attenzione alla sezione bullismo e cyberbullismo, Regolamento di disciplina, Piano dell'offerta formativa triennale, ecc.) contengono una o più sezioni nelle quali sono esplicitati diritti e doveri degli operatori scolastici, degli alunni e dei genitori o di coloro che esercitano la responsabilità genitoriale. Tali documenti sono pubblicati sul sito dell'Istituto.

Il genitore, sottoscrivendo l'istanza d'iscrizione, assume l'impegno di:

- a) osservare le disposizioni contenute nel Patto di corresponsabilità e nel Regolamento d'Istituto;
- b) sollecitarne l'osservanza da parte dello studente.

Il genitore è consapevole che:

- a) le infrazioni disciplinari da parte dell'alunno possono dar luogo a sanzioni disciplinari;

b) in caso di danneggiamenti o lesioni a persone, la sanzione è ispirata al principio della riparazione del danno (art. 4, comma 5 del DPR 249/1998, come modificato dal DPR 235/2007);

c) il Regolamento d'Istituto disciplina le modalità d'irrogazione delle sanzioni disciplinari e i mezzi d'impugnazione verso i provvedimenti disciplinari.

All'inizio dell'anno scolastico, in occasione della presentazione del Regolamento d'Istituto agli alunni da parte dei docenti, verrà analizzata la ePolicy d'Istituto. Nel corso dell'anno ogni docente dedicherà alcune lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo (anche nell'ambito delle attività di Educazione civica).

---

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

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

Nelle attività scolastiche ed extra-scolastiche gli studenti assumono i comportamenti richiesti dalle norme giuridiche, dallo Statuto delle studentesse e degli studenti e dal Regolamento di Istituto.

Il Regolamento d'Istituto, e, in particolare, la Sezione IV "Regolamento disciplinare", nel rispetto della normativa vigente, individuano i comportamenti che configurano mancanze disciplinari, le relative sanzioni, gli organi competenti a irrogarle e il relativo procedimento.

I provvedimenti disciplinari hanno finalità educativa, tendono al rafforzamento del senso di responsabilità e al ripristino di rapporti corretti all'interno della scuola e sono ispirati, per quanto possibile, al principio della riparazione del danno.

Le infrazioni disciplinari sono specificate nell'apposita tabella contenuta nella Sezione IV "Regolamento disciplinare", che indica altresì le sanzioni in caso di prima infrazione, le sanzioni in caso di aggravanti, le infrazioni in caso di comportamenti reiterati e l'organo competente a comminare le sanzioni.

In nessun caso può essere sanzionata, né direttamente né indirettamente, la libertà di espressione, qualora sia correttamente manifestata e non lesiva dell'altrui dignità e personalità. La responsabilità disciplinare è personale.

Nessuno può essere sottoposto a sanzioni disciplinari senza essere stato prima invitato a esporre le proprie ragioni. Lo studente ha facoltà di produrre testimonianze o elementi di prova a sé favorevoli.

Le sanzioni disciplinari sono sempre temporanee, proporzionate all'infrazione disciplinare, graduale e devono tenere conto della situazione personale dello studente. Tutti i provvedimenti che infliggono sanzioni disciplinari devono essere motivati oralmente e/o per iscritto.

Per quanto possibile, allo studente sarà offerta da parte dell'organo competente all'irrogazione, la possibilità di convertire la sanzione disciplinare in attività a favore della collettività, ossia socialmente utili. In caso di danni materiali, il responsabile o i genitori sono tenuti al risarcimento.

In merito ai provvedimenti disciplinari, il Regolamento d'Istituto indica i mezzi

di impugnazione (come il ricorso all'organo di Garanzia interno alla scuola) e i termini da rispettare.

A seconda dell'età degli studenti e in base alla gravità e alla diffusione di comportamenti devianti, si valuterà un intervento su tutto il contesto classe, con attività educative e di sensibilizzazione, anche per promuovere una maggior consapevolezza circa l'utilizzo delle TIC e di Internet. Si valuterà altresì l'opportunità di coinvolgere nell'azione educativa e formativa anche altri soggetti (psicologo scolastico, Rete di scuole, Polizia postale ecc.).

Anche nei confronti del personale scolastico possono essere adottati provvedimenti disciplinari, in caso di uso improprio di dispositivi digitali e della Rete, o in caso non intervenga o non segnali gravi comportamenti scorretti tenuti dagli studenti.

---

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

Il Regolamento d'Istituto 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.

Il Dirigente scolastico, in collaborazione con i Referenti bullismo e cyberbullismo, valuterà la necessità di aggiornare periodicamente il Regolamento d'Istituto con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida del Ministero dell'Istruzione e le indicazioni normative generali.

Il Regolamento d'Istituto disciplina in modo dettagliato le tematiche in oggetto, e in particolare:

- la Sezione II si occupa di regolare l'uso dei dispositivi elettronici e dei telefonicellulari;
- la Sezione III contiene un Regolamento specifico sul bullismo e il cyberbullismo.

Il personale scolastico si impegna a conoscere e ad applicare il Regolamento d'Istituto e gli eventuali aggiornamenti. A tale scopo partecipa periodicamente ad attività formative in materia di privacy e di utilizzo corretto dei dispositivi digitali.

---

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

L'E-policy viene aggiornata periodicamente, soprattutto 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 Dirigente scolastico, in collaborazione con i docenti referenti per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo, valuterà periodicamente la necessità di procedere alla revisione e all'aggiornamento dell'ePolicy.

Il monitoraggio dell'implementazione della ePolicy avverrà:

- all'inizio dell'anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dei Referenti per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo, dell'Animatore digitale e del Team per l'innovazione digitale, della Funzione strumentale PTOF;
- alla fine di ogni anno scolastico, contestualmente al Rapporto di Autovalutazione e sulla base dei casi problematici riscontrati.

Il mondo digitale è in continua evoluzione, e alcuni dei cambiamenti che sono già in atto, si prospettano come delle nuove "rivoluzioni digitali". Si pensi al Metaverso, ai nuovi spazi virtuali frequentati da "avatar", agli NFT (non-fungible token) ecc. Questi cambiamenti sono monitorati continuamente all'interno del nostro Istituto, e si studiano anche le possibili implicazioni, positive e negative, che tali innovazioni potranno avere in generale, e sul mondo della scuola in particolare.

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

---

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

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti

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

- 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 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 curricolo

### 2.1. Curricolo sulle competenze digitaliper gli studenti

I ragazzi usano quotidianamente la Rete e i dispositivi digitali, 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 l'Istituto 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 curricolo digitale.

L'Istituto Mattei propone un curricolo che punta all'acquisizione e allo sviluppo delle competenze digitali degli studenti, con particolare riguardo al pensiero computazionale e all'utilizzo critico e consapevole della Rete e dei social network, al potenziamento delle metodologie laboratoriali e delle attività di laboratorio, alla prevenzione e contrasto dei comportamenti devianti.

Per questo l'Istituto 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 avviene attraverso la progettazione e implementazione di un curricolo digitale, continuativo e trasversale alle varie discipline.

L'Animatore digitale assume un ruolo strategico nella promozione dell'innovazione, sia attraverso il coinvolgimento della comunità scolastica in azioni formative, sia attraverso la creazione di soluzioni didattiche, laboratoriali, metodologiche e tecnologiche.

L'Istituto Mattei è scuola - capofila del Labcommunity, che vede coinvolti molteplici partner (Università, Start up, imprese, terzo settore, scuole ed Amministrazioni locali) nella creazione e fruizione di spazi ad alta tecnologia (fabbricazione digitale, stampa 3D, taglio laser, Arduino, modellazione CAD, ecc.).

Diverse sono le iniziative di ampliamento curricolare previste dal PTOF d'Istituto:

- ECDL: conseguimento della patente europea, che permette l'acquisizione delle abilità di base per l'uso del computer. Promozione delle competenze informatiche di studenti e del personale della scuola, nonché di esterni ad essa.
- CORSO AUTOCAD 2D: conseguimento della certificazione Autodesk Certified Autodesk:
- CLASSE 2.0 NEL BIENNIO: Classi digitali con utilizzo di setting innovativi. Il progetto intende promuovere un uso consapevole delle nuove tecnologie digitali ed una maggiore

- motivazione, grazie a metodologie attive e cooperative.
- L'UNIVERSO DIETRO UN CLICK - PREVENZIONE DEL CYBERBULLISMO E DEL SEXTING. Il progetto è rivolto agli studenti delle classi seconde e terze, ha l'intento di sviluppare le life skills, di prevenire bullismo, cyberbullismo, sexting, di sviluppare il benessere e il rispetto per se stessi e gli altri, di promuovere azioni di peer-education.
- BEN-ESSERE A SCUOLA: diversi interventi orientati a prevenire la dispersione scolastica e a promuovere il benessere integrale dello studente, mediante la sinergica collaborazione con altri Enti del Territorio.
- EDUCAZIONE ALLA LEGALITÀ E PREVENZIONE AI FENOMENI DI BULLISMO E CYBERBULLISMO: mediante la collaborazione con diversi soggetti esterni (Polizia postale, Arma dei carabinieri, Università, Avvocati penalisti, Enti locali, ecc.), si intendono sviluppare competenze di cittadinanza attiva.
- MONITORAGGIO SUI FENOMENI DI BULLISMO E CYBERBULLISMO: gli studenti e i docenti del nostro Istituto partecipano periodicamente al monitoraggio organizzato dal Ministero dell'Istruzione in collaborazione con l'Università di Firenze.

Le competenze digitali richiamano diverse dimensioni sulle quali è 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 gli studenti sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana;
- 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 l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità sociocomunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

Premesso ciò, è opportuno fare riferimento ad un framework comune per le competenze digitali e l'educazione ai media degli studenti. I documenti che sono stati considerati per progettare e implementare il curricolo sulle competenze digitali sono:

- Piano Scuola Digitale (PNSD), in particolar modo il paragrafo 4.2. su "Competenze e contenuti";
- Sillabo sull'Educazione Civica Digitale: ha lo scopo di inquadrare temi e contenuti che sono alla base dello sviluppo di una piena cittadinanza digitale degli studenti attraverso il percorso educativo;
- DigComp 2.2.: "Il quadro di riferimento per le competenze digitali dei cittadini" (European Digital Competence Framework for Citizens), il documento che contiene le linee guida per l'Educazione Digitale con livelli di padronanza ed esempi di utilizzo;
- Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente (C189/9, p. 9).

Il curriculum d'Istituto sulle competenze digitali si basa sulle aree di competenza individuate dal Digcomp che sono, nello specifico:

**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 punta a sviluppare negli studenti 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.

**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".

**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. 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.

**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, si punta a sviluppare negli studenti 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.

## **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 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 e critico delle nuove tecnologie e per armonizzare gli apprendimenti.

La professione docente è complessa e pertanto richiede competenze diverse ed integrate, fra queste anche quelle di tipo digitale. Nell'Istituto Mattei, le TIC sono utilizzate dai docenti ad integrazione della didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli studenti e le studentesse della classe, anche delle persone con disabilità (in chiave inclusiva). In generale, gli insegnanti hanno raggiunto un buon livello di formazione in merito all'utilizzo e l'integrazione delle TIC nella didattica.

L'Istituto, attraverso il Collegio dei docenti, riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (ad es. con l'aiuto dell'Animatore digitale), dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti, purché restino coerenti con il Piano di formazione. Periodicamente vengono organizzate attività di formazione che promuovono l'uso delle TIC nella didattica: 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. Inoltre, le attività di formazione organizzate dalla scuola 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. La competenza digitale, oggi, è imprescindibile per i docenti, così come per studenti e studentesse e permette, di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento.

---

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

L'Istituto Mattei si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avviene tramite specifici percorsi di aggiornamento che, con cadenza, verranno organizzati dall'Istituto 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, ecc.), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti sul territorio.

Al fine di creare ulteriore sinergia fra scuola, studenti e famiglie, di promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo, il Dirigente scolastico, i docenti membri del Team antibullismo e gli altri insegnanti interessati, seguono percorsi formativi specifici che hanno ad oggetto l'uso responsabile e sicuro delle nuove

tecnologie e i rischi legati alla Rete (ad esempio il corso organizzato dal Ministero dell'istruzione, in collaborazione con l'Università di Firenze, tramite la Piattaforma Elisa; corsi sulla privacy, ecc.).

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 che usano le nuove tecnologie. Essi, 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 educarli alle emozioni in un contesto on-line e per modulare e gestire i propri ed altrui comportamenti, favorendo e promuovendo forme di convivenza civile.

I momenti di formazione e aggiornamento sono pensati e creati anche in base all'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica (compilazione di questionario sui bisogni formativi).

E' stata predisposta un'area specifica sul cloud d'Istituto con materiali formativi per gli insegnanti in merito a diverse tematiche attinenti alle nuove tecnologie: bullismo e cyberbullismo, privacy, didattica digitale integrata, ecc. Nella sezione, sono stati pubblicati materiali utili per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet e materiali informativi del progetto "Generazioni connesse", a partire dall'inserimento del link del progetto: [www.generazioniconnesse.it](http://www.generazioniconnesse.it), che consente di consultare ulteriori materiali di aggiornamento e di approfondimento.

---

#### **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 gli studenti verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto Mattei garantisce la massima informazione alle famiglie in merito alle 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.

Oggi più che mai è importante rinforzare l'alleanza educativa fra scuola e famiglie. L'Istituto Mattei persegue il coinvolgimento delle famiglie nell'educazione digitale degli studenti e delle studentesse, con attività di formazione, che permettono di coinvolgere e sensibilizzare anche i genitori.

Il "Patto di corresponsabilità" dell'Istituto Mattei è contenuto nel Titolo XVIII del Regolamento d'Istituto e prevede specifici riferimenti alle tecnologie digitali.

In merito agli impegni assunti dai genitori, nel Patto di Corresponsabilità dell'Istituto Mattei si indicano anche i seguenti:

- instaurare un dialogo costruttivo con l'Istituzione scolastica;
- contattare i figli durante l'orario scolastico tramite la segreteria e non tramite il telefono cellulare;
- partecipare attivamente alle azioni di formazione/informazione,

- promosse dall'Istituto aventi a oggetto bullismo e cyberbullismo;
- vigilare sui comportamenti dei propri figli, in particolar modo sull'uso delle tecnologie digitali;
  - prendere conoscenza delle azioni messe in campo dalla scuola e collaborare secondo le modalità previste dal Patto di corresponsabilità;
  - prendere conoscenza della sezione disciplinare e della sezione bullismo e cyberbullismo del Regolamento di Istituto;
  - segnalare al Coordinatore di classe o alla Presidenza i comportamenti devianti e gli eventuali episodi di bullismo o cyberbullismo che coinvolgano i propri figli o altri studenti dell'Istituto, sia come vittime sia come autori di atti di bullismo o cyberbullismo, di cui vengono a conoscenza, direttamente o indirettamente, al fine di coinvolgere gli organi scolastici competenti (Consiglio di Classe, Dirigente scolastico o Consiglio di Istituto).

Per chiarire meglio il percorso di revisione del "Patto di Corresponsabilità", il Ministero dell'istruzione 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 dividerne i contenuti e a rispettarne gli impegni".

## **Il nostro Piano d'azioni**

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

- 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.
- 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.

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

- 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.

L'art. 8 della Carta dei diritti fondamentali dell'Unione europea considera la protezione dei dati personali come un diritto fondamentale dell'individuo. Tale diritto è tutelato anche dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio dell'UE, del 27 aprile 2016 (relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla circolazione di tali dati). Anche le istituzioni scolastiche hanno l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D. Lgs. 10 agosto 2018, n. 101.

In questo paragrafo dell'ePolicy si affronta tale problematica, con particolare riferimento all'uso delle tecnologie digitali, e indichiamo le misure che l'Istituto Mattei attua per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione agli studenti. 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.

In particolare, l'Istituto Mattei non solo garantisce la tutela dei dati personali e sensibili degli studenti e delle loro famiglie, ma anche si impegna ad informare e soprattutto a rendere consapevoli gli studenti di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

Il personale scolastico partecipa a specifici percorsi formativi, in modo da assicurare il trattamento dei dati personali e sensibili nel rispetto della normativa vigente.

I genitori sono tenuti a compilare le seguenti autorizzazioni al trattamento dei dati personali:

<https://matteirho.edu.it/wp-content/uploads/2020/11/Mod-A-196-AUTORIZZAZIONE-TRATTAMENTO-DATI-1.pdf>

<https://matteirho.edu.it/wp-content/uploads/2021/06/Modello-autorizzazione-immagine.pdf>

Tali modelli sono stati aggiornati in base ai provvedimenti normativi più recenti: Regolamento (UE) 2016/679 e D. Lgs. 10 agosto 2018, n. 101.

---

### **3.2 - Accesso ad Internet**

1. L'accesso a Internet è un diritto fondamentale della persona e una 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.

Per quanto riguarda l'accesso alla Rete, l'Istituto Mattei dispone di una connessione a Internet in fibra e a banda ultra-larga. Si è provveduto al cablaggio interno di tutti gli spazi della scuola (LAN/W-Lan). Sono state configurate diverse reti WIFI per consentire l'accesso alle diverse tipologie di utenti:

- Matteiwifi per i docenti
- MatteiLIM-NBooks per le LIM nelle classi
- Guest

L'autorizzazione all'accesso alla rete WIFI dell'istituto viene concessa a tutto il personale in servizio, agli studenti delle classi digitali e a quelli che ne fanno richiesta per esigenze legate allo svolgimento di particolari attività/progetti. L'accesso viene consentito anche a personale esterno che

svolge specifiche attività all'interno dell'istituto (es. esperti esterni, educatori, ecc.).

L'Istituto è registrato alla piattaforma Microsoft Office 365, con canone annuo a carico della scuola: questo consente ai destinatari di utilizzare le funzionalità dell'ambiente online Off365, per il lavoro collaborativo nelle classi, e di scaricare e utilizzare in locale il pacchetto MS Office 2016.

E' stato adottato un Sistema di Autenticazione unica (Single-Sign-On): l'obiettivo è di adottare un unico sistema di riconoscimento con cui un utente possa accedere a tutte le risorse e i servizi a cui è abilitato. Questo permette un accesso controllato e sicuro ai servizi digitali offerti dalla scuola e dalla rete.

L'Istituto Mattei dispone di 5 laboratori d'informatica, di cui 2 mobili. Ogni aula è dotata di monitor interattivo collegato alla Rete. Sono a disposizione di docenti e studenti anche 120 computer portatili.

E' stato conseguito anche l'obiettivo di una vera e propria "amministrazione digitale", attraverso la completa digitalizzazione della segreteria scolastica, che permette la conservazione sostitutiva dei documenti della scuola, la gestione del fascicolo elettronico degli utenti, l'archivio virtuale e la tutela dei dati personali.

Il Regolamento d'Istituto dedica alcune sezioni all'uso delle TIC. L'Istituto Mattei ha adottato in questo modo una "Politica di Uso Accettabile delle tecnologie a scuola" (PUA). Il Titolo II del Regolamento disciplina le Comunicazioni scuola-famiglia e dedica due sezioni alle Modalità di comunicazione e alle Comunicazioni tra docenti e studenti tramite chat, e-mail, social media ecc. Il Titolo VI "Disciplina degli alunni" dedica la Sezione II all'uso dei telefoni cellulari e dispositivi elettronici e la Sezione III al Regolamento sul bullismo e il cyberbullismo. In particolare, la Sezione II, in linea con quanto stabilito dalla Direttiva ministeriale del Miur n° 30 del 15/03/2007 avente ad oggetto: "Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti", stabilisce quanto segue:

- il divieto di utilizzo del cellulare o di altri dispositivi elettronici durante le ore di lezione risponde a una generale norma di correttezza nei confronti dei docenti e dei compagni di classe e trova una sua codificazione formale nei doveri indicati nello Statuto delle studentesse e degli studenti;
- l'utilizzo non autorizzato del cellulare o di altri dispositivi elettronici costituisce un'infrazione disciplinare sanzionabile nelle forme stabilite dal Regolamento di disciplina dell'Istituto (ivi compreso il ritiro temporaneo del cellulare durante le ore di lezione);
- resta fermo che, anche durante lo svolgimento delle attività didattiche, eventuali esigenze di comunicazione tra gli studenti e le famiglie, dettate da ragioni di particolare urgenza o gravità, potranno sempre essere soddisfatte, previa autorizzazione dei Docenti in servizio, della Vicepresidenza o della Presidenza;
- il divieto di utilizzare telefoni cellulari durante lo svolgimento di attività di insegnamento apprendimento, del resto, opera anche nei confronti del personale docente (cfr. Circolare n. 362 del 25 agosto 1998 e doveri derivanti dal CCNL), in considerazione della necessità di assicurare all'interno della comunità scolastica le migliori condizioni per uno svolgimento sereno ed efficace delle attività didattiche, unitamente all'esigenza educativa di offrire ai discenti un modello di riferimento esemplare da parte degli adulti;
- il divieto di effettuare chiamate tramite telefoni cellulari opera

anche nei confronti dei genitori e dei familiari o amici dello studente che non deve essere disturbato durante le ore di lezione. Eventuali comunicazioni di fatti urgenti o di estrema gravità potranno avvenire tramite la Segreteria didattica, la Vice Presidenza o la Presidenza dell'Istituto.

- l'utilizzo del cellulare o di altri dispositivi elettronici durante le ore di lezione da parte di Studenti e Docenti è consentito solo per lo svolgimento di attività didattiche;
- l'obbligo da parte di studenti, familiari, docenti e personale A.T.A. di comunicare alla Presidenza o alla Vice –Presidenza l'uso improprio di telefoni cellulari e apparecchiature elettroniche in particolar modo per effettuare riprese video non autorizzate durante le ore di lezione e comunque nelle varie pertinenze dell'Istituto, all'insaputa o a danno di altri studenti o Docenti; vige anche l'obbligo di segnalare la pubblicazione di riprese video non autorizzate, anche sui social media.

L'ePolicy è il documento in cui in modo discorsivo e generale vengono descritti gli aspetti necessari per dotarsi di una visione e comprensione del fenomeno e delle sue potenzialità in ambito didattico; le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali. Nel Regolamento d'Istituto sono elencate in modo puntuale le regole di ingaggio nell'utilizzo della strumentazione tecnologica della scuola, ovvero le azioni che docenti, personale scolastico e studenti possono e non possono compiere quando si connettono alla Rete e/o accedono a un device.

Il Regolamento d'Istituto dedica una sezione all'uso dei dispositivi personali a scuola e, in particolare, nel corso delle attività didattiche. E' prevista la metodologia BYOD: il docente può autorizzare gli studenti ad utilizzare il proprio device durante le lezioni (tablet, PC o smartphone). Il PTOF dell'Istituto Mattei prevede l'attivazione di classi digitali nel primo biennio e l'insegnamento dell'Informatica in quasi tutti gli indirizzi, in particolare nell'articolazione SIA, Sistemi informativi e aziendali.

L'Istituto Mattei è già dotato dunque di una PUA (Politica d'Uso Accettabile), contenuta nel Regolamento d'Istituto. Il Regolamento elenca i seguenti doveri degli studenti:

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  
utilizzare i propri device in modo sicuro, proteggendoli con password efficaci, da aggiornare periodicamente, in modo da evitare diffusioni di dati riservati e personali.

L'Istituto Mattei assicura l'impiego di tutte le misure necessarie per garantire agli studenti l'accesso a materiale appropriato. Allo stesso tempo la scuola non può essere responsabile per l'accesso autonomo da parte degli studenti a materiali inadeguati e potenzialmente dannosi trovati online. Il curriculum scolastico prevede che gli studenti imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le ICT. Ma ciò non è sufficiente: è anche fondamentale dotare gli studenti/esse delle competenze necessarie ad affrontare la complessità del mondo dell'informazione, che ormai richiede di essere in grado di destreggiarsi tra notizie e fake news, discussioni online e discorsi d'odio (hate speech).

La scuola fornisce al personale e agli studenti un indirizzo di posta elettronica personale, attivo per il tempo di permanenza nell'Istituto: l'indirizzo si può utilizzare per accedere alle piattaforme e-learning (Teams) e tutte le altre attività ICT della scuola. E' prevista la scadenza programmata dell'account al 31 agosto dell'anno di fine percorso scolastico per gli studenti e di fine servizio per il personale scolastico (ad esempio per il personale assunto con contratto a tempo determinato).

E' stato predisposto uno spazio di cloud computing (Microsoft 365 e Teams): questo ha consentito una riduzione dei costi e una maggiore efficienza nell'archiviazione della documentazione e della modulistica. Sono stati attivati account personali per l'accesso a queste piattaforme e un indirizzo mail per il personale e per gli studenti. Questi interventi facilitano le comunicazioni tra docenti e studenti e le attività didattiche. Particolare attenzione è stata riservata al trattamento dei dati personali.

Si adotta la seguente 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 standby, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate;
- Programmare l'eliminazione periodica di dati di navigazione, password inutilizzate ad eventuali documenti personali memorizzati;
- 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, ecc.);
  - 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 on line**

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.

Le nuove tecnologie facilitano e migliorano la comunicazione: per questo all'interno dell'Istituto Mattei si utilizzano diversi strumenti di comunicazione online. A tale proposito è importante effettuare una distinzione preliminare fra comunicazione interna e comunicazione esterna. La scuola utilizza diversi strumenti di comunicazione on-line, sia per far circolare all'interno della scuola informazioni di servizio o contenuti importanti fra i diversi attori scolastici (docenti, studenti, genitori, collaboratori scolastici ecc.), sia per raggiungere target esterni, al fine di valorizzare e promuovere le attività portate avanti dall'Istituto (rivolgendosi ad esempio a istituzioni, famiglie, studenti non ancora iscritti, associazioni ecc.).

Fra gli strumenti di comunicazione esterna, troviamo il sito web della scuola (che viene continuamente aggiornato e che contiene tutti i link alle diverse applicazioni che si utilizzano nelle diverse attività istituzionali: Registro elettronico, Circolari, ecc.), profili sui social network (Facebook, Youtube, Instagram), il notiziario on line d'Istituto ("La testata del Mattei"). Tali strumenti sono utilizzati anche per fornire informazioni di servizio rivolte a studenti o genitori. La comunicazione esterna online della scuola è coordinata e progettata in base al Piano di comunicazione d'Istituto e permette di trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che l'Istituto promuove. La comunicazione esterna dell'Istituto è progettata ed implementata anche con il supporto degli studenti che producono contenuti multimediali da diffondere attraverso i vari canali in uso (articoli sul notiziario d'Istituto, video, foto, post sui social, articoli per il sito ecc.).

Fra gli strumenti di comunicazione interna, invece, troviamo il Registro elettronico con tutte le sue funzionalità, la posta elettronica ordinaria, applicativi e piattaforme di lavoro condiviso e collaborativo come Microsoft Teams che sono utilizzati anche per facilitare e rendere più partecipata la didattica e la comunicazione a scuola. Gli strumenti di messaggistica istantanea, come Whatsapp, sono utilizzati solo per le comunicazioni informali tra docenti. Per quanto riguarda le comunicazioni istituzionali con il personale scolastico è garantito il "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare.

In merito alle "Comunicazioni tra docenti e studenti tramite chat, e-mail, social media ecc.", l'art. 2.2 del Titolo II del Regolamento d'Istituto prevede che "Al personale dell'Istituto in servizio è consentito di comunicare via chat, e-mail, telefono o social media ecc. con gli studenti in corso esclusivamente per svolgere od organizzare attività di natura puramente didattica. E' fatto

assoluto divieto di pubblicare audio, video, immagini e materiali didattici senza il previo consenso delle parti interessate. Chiunque venga a conoscenza di attività espressamente vietate dalla legge o dal presente Regolamento è tenuto a darne comunicazione alla Presidenza o alla Vice-Presidenza dell'Istituto”.

Per le chat informali fra membri del personale scolastico, si propone di elaborare un sistema di regole condivise:

- mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- rispettare il segreto d'ufficio;
- non diffondere dati personali, dati sensibili e immagini senza il consenso dell'interessato;
- utilizzare un linguaggio corretto e non ricorrere ad espressioni ingiuriose o diffamatorie lesive della dignità altrui.

Il Registro elettronico (Axios) è lo strumento che i docenti devono utilizzare per la gestione di assenze, presenze, valutazioni, prenotazioni di incontri e comunicazioni con le famiglie. Il Registro elettronico permette di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su:

- andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
- risultati scolastici (voti, documenti di valutazione);
- udienze (prenotazioni colloqui individuali);
- eventi (agenda eventi);
- comunicazione varie (comunicazioni di classe, comunicazioni personali).

Il Regolamento d'Istituto regola l'utilizzo del Registro elettronico da parte del personale scolastico e da parte degli studenti e dei genitori.

---

### **3.4 - Strumentazione personale**

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli studenti 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 indicati dal Ministero dell'istruzione 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.

Presso l'Istituto Mattei, la strumentazione tecnologica personale viene utilizzata come integrazione della didattica. I docenti possono utilizzare dispositivi personali per avvicinare gli studenti e le studentesse alle discipline e per facilitare lo studio nella sua organizzazione complessiva.

Nel DPR 24 giugno 1998, n. 249 "Regolamento recante lo Statuto delle studentesse e degli studenti della scuola secondaria" (in GU 29 luglio 1998, n. 175), all'art. 2 (sezione Diritti), punto 8, lettera e, si sottolinea "la disponibilità di un'adeguata strumentazione tecnologica" di cui la scuola deve dotarsi per offrirla ai propri studenti e alle studentesse che, d'altra parte, "sono tenuti ad avere nei confronti del capo d'istituto, dei docenti, del personale tutto della scuola e dei loro compagni lo stesso rispetto, anche formale, che chiedono per se stessi" (Art. 3, punto 2 sezione Doveri).

Si ricordano alcuni doveri che gli studenti devono rispettare e che sono previsti dall'art. 3 del DPR n. 249/1998:

non utilizzare il telefono cellulare, o altri dispositivi elettronici, durante lo svolgimento delle attività didattiche, considerato che il discente ha il dovere:

- assolvere assiduamente agli impegni di studio anche durante gli orari di lezione (comma 1);
- tenere comportamenti rispettosi degli altri (comma 2), nonché corretti e coerenti con i principi di cui all'art. 1 (comma 3);
- osservare le disposizioni organizzative dettate dai regolamenti di istituto (comma 4)" (DM n. 30 del 15/03/2007 "Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, doveri di vigilanza e di corresponsabilità dei genitori e dei docenti").

La Sezione II del Regolamento d'Istituto è dedicata all'uso dei telefoni cellulari e dei dispositivi elettronici. In linea con quanto stabilito dalla Direttiva ministeriale del Miur n° 30 del 15/03/2007 avente ad oggetto: "Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti", si specifica quanto segue:

il divieto di utilizzo del cellulare o di altri dispositivi elettronici durante le ore di lezione risponde a una generale norma di correttezza nei confronti dei docenti e dei compagni di classe e trova una sua codificazione formale nei doveri indicati nello Statuto delle studentesse e degli studenti;

l'utilizzo non autorizzato del cellulare o di altri dispositivi elettronici costituisce un'infrazione disciplinare sanzionabile nelle forme stabilite dal Regolamento di disciplina dell'Istituto (ivi compreso il ritiro temporaneo del cellulare durante le ore di lezione);

resta fermo che, anche durante lo svolgimento delle attività didattiche, eventuali esigenze di comunicazione tra gli studenti e le famiglie, dettate da ragioni di particolare urgenza o gravità, potranno sempre essere soddisfatte, previa autorizzazione dei Docenti in servizio, della Vicepresidenza o della Presidenza;

il divieto di utilizzare telefoni cellulari durante lo svolgimento di attività di insegnamento apprendimento, del resto, opera anche nei confronti del personale docente (cfr. Circolare n. 362 del 25 agosto 1998 e doveri derivanti dal CCNL), in considerazione della necessità di assicurare all'interno della comunità scolastica le migliori condizioni per uno svolgimento sereno ed efficace delle attività didattiche, unitamente all'esigenza educativa di offrire ai discenti un modello di riferimento esemplare da parte degli adulti;

il divieto di effettuare chiamate tramite telefoni cellulari opera anche

nei confronti dei genitori e dei familiari o amici dello studente che non deve essere disturbato durante le ore di lezione. Eventuali comunicazioni di fatti urgenti o di estrema gravità potranno avvenire tramite la Segreteria didattica, la Vice Presidenza o la Presidenza dell'Istituto.

l'utilizzo del cellulare o di altri dispositivi elettronici durante le ore di lezione da parte di Studenti e Docenti è consentito solo per lo svolgimento di attività didattiche;

l'obbligo da parte di studenti, familiari, docenti e personale A.T.A. di comunicare alla Presidenza o alla Vice –Presidenza l'uso improprio di telefoni cellulari e apparecchiature elettroniche in particolar modo per effettuare riprese video non autorizzate durante le ore di lezione e comunque nelle varie pertinenze dell'Istituto, all'insaputa o a danno di altri studenti o Docenti; vige anche l'obbligo di segnalare la pubblicazione di riprese video non autorizzate, anche sui social media.

L'utilizzo del proprio dispositivo da parte degli studenti è consentito, nel caso della metodologia BYOD, qualora i docenti proponessero ai propri studenti l'uso di device personali (tablet, PC o smartphone) in classe. Inoltre il PTOF d'Istituto prevede l'attivazione di classi digitali nel primo biennio e l'insegnamento dell'Informatica in quasi tutti gli indirizzi, in particolare nell'articolazione SIA, Sistemi informativi e aziendali.

Il Regolamento d'Istituto provvede altresì ad elencare i comportamenti scorretti nell'utilizzo dei dispositivi digitali e le sanzioni corrispondenti. Questo tema è disciplinato anche nel Patto educativo di corresponsabilità, che si occupa di condividere diritti e doveri fra scuola e famiglia.

A tale scopo, il Ministero dell'Istruzione, in collaborazione con AGID (l'Agenzia per il Digitale) e il Garante per la Privacy, ha elaborato apposite Linee guida per promuovere l'utilizzo corretto della strumentazione personale a scuola. L'Istituto Mattei recepisce queste indicazioni, che costituiscono un vero e proprio decalogo (i dieci i punti del Ministero dell'istruzione per l'uso dei dispositivi mobili a scuola, BYOD - "Bring your own device"):

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;

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;

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;

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;

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; 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;

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;

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. 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; 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;

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.

L'Istituto Mattei, aderendo al progetto Generazioni Connesse, si impegna a sensibilizzare, formare e responsabilizzare tutti i soggetti che partecipano al processo educativo e didattico. L'utilizzo delle tecnologie e dei dispositivi anche personali va mediato e calibrato, anche al fine di favorire negli studenti lo sviluppo di un pensiero critico. L'ePolicy, documento di indirizzo e programmazione interno al progetto, viene redatto per perseguire tali obiettivi, per potenziare le competenze di cittadinanza digitale e per favorire un utilizzo costruttivo e consapevole del proprio dispositivo (azione #15 del PNSD - Scenari innovativi per lo sviluppo di competenze digitali applicate).

### ***Il nostro Piano d'azioni***

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- 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 uno o più eventi o attività volti a formare il personale 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 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).**

- 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 uno o più eventi o attività volti a formare il personale 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 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 pericolose. 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:

- Interventi di 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.
- Interventi di 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.

I rischi online sono diversi, soprattutto in caso di utilizzo non responsabile delle tecnologie digitali da parte degli studenti: adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia (recenti ricerche hanno sottolineato come la maggior parte degli adolescenti reperisca in Rete informazioni inerenti la sessualità, col rischio, spesso effettivo, del diffondersi di informazioni scorrette e/o dell'avvalorarsi di falsi miti), pedopornografia (con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone minorenni), gioco d'azzardo o gambling, videogiochi online (alcuni rischi associati possono essere: contatti impropri con adulti, contenuti violenti e/o inadeguati; acquisti incontrollati, ecc.), esposizione a contenuti dannosi o inadeguati (es. hate speech, contenuti razzisti, messaggi che inneggiano al suicidio, a competizioni pericolose, che promuovono comportamenti alimentari scorretti, ecc.).

L'Istituto Mattei si impegna a promuovere costantemente negli studenti le necessarie competenze e capacità, al fine di una protezione adeguata, ma anche al fine di un utilizzo consapevole che permetta di sfruttare le potenzialità delle tecnologie digitali e di gestirne le implicazioni.

Per perseguire questi obiettivi, la scuola organizza periodicamente interventi di sensibilizzazione e di formazione che hanno come obiettivo quello di innescare e promuovere un cambiamento. Queste attività destinate alle singole classi o a tutti gli studenti, presentano diversi benefici, quali:

- accrescere la consapevolezza negli studenti sull'utilizzo corretto delle nuove tecnologie e sui rischi della Rete e i comportamenti devianti;
- incoraggiare il gruppo a modificare i propri comportamenti;
- diffondere all'esterno del gruppo di riferimento e quindi in tutta la comunità scolastica questa consapevolezza;
- facilitare il coinvolgimento di altri soggetti (studenti più piccoli, genitori ecc.);
- favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva.

Oltre a queste attività di sensibilizzazione, l'Istituto Mattei si impegna a predisporre opportuni interventi e strumenti di prevenzione, con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale. Se il problema della "sicurezza" è difficilmente riconducibile esclusivamente all'esistenza in sé di alcuni rischi, più o meno gravi e insidiosi, appare chiaro dunque come le migliori strategie di intervento siano di carattere prevalentemente preventivo. Le attività di prevenzione sono organizzate in modo permanente dalla scuola, sono previste dal PTOF d'Istituto e sono rivolte a tutti gli studenti (prevenzione universale). Altri interventi sono predisposti per tutte quelle situazioni specifiche che lo richiedono, ad esempio per episodi di bullismo e cyberbullismo o per studenti non adeguatamente scolarizzati (prevenzione selettiva e prevenzione indicata).

La "prevenzione universale" si riferisce ad un programma che parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti a tutti gli studenti o a gruppi della popolazione scolastica che non sono stati identificati sulla base del rischio individuale.

La "prevenzione selettiva" è dedicata 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 contesto. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali. Può essere un valido programma per quelle situazioni in cui la prevenzione universale non ha dato gli esiti previsti.

La "prevenzione indicata" consiste, infine, in un programma di intervento sul caso specifico, pensato e strutturato per adattarsi agli studenti con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime.

Il modello diviso in tre livelli può essere un'utile guida per affrontare e prevenire ogni possibile situazione di disagio. E' tuttavia comprensibile la difficoltà di poter strutturare soluzioni ed interventi multilivello da parte di un'istituzione scolastica senza il supporto di altri attori. Per questo, oltre ad attività formative destinate al personale scolastico in generale, l'Istituto Mattei ha provveduto ad organizzare attività formative specifiche per alcuni docenti (docenti del Team antibullismo), collabora con professionisti diversi (psicologo scolastico, Forze dell'ordine, enti che operano sul territorio ecc.), partecipa alla Rete di scuole Ri-connect. Infine, nel rispetto del Patto di corresponsabilità e della propria funzione educativa, anche i genitori sono chiamati a partecipare agli interventi di sensibilizzazione e di prevenzione organizzati dalla scuola.

---

#### **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.
- 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).

Il bullismo è costituito da un insieme di atti aggressivi, compiuti da un individuo o da un gruppo, ripetutamente e nel tempo, contro una vittima che non riesce a difendersi. Il bullismo presenta tre requisiti sostanziali:

- l'intenzionalità del comportamento offensivo e aggressivo;
- la continuità temporale dello stesso;
- il rapporto “asimmetrico” tra il bullo e la vittima.

Tra le forme di manifestazione del bullismo, sono emerse:

- quella diretta, cioè la violenza fisica;
- quella indiretta, che si esplica nella violenza verbale e psicologica, spesso preordinata ad isolare la vittima.

Il cyberbullismo presenta questi caratteri tipici:

- l'intenzionalità del comportamento offensivo e aggressivo;
- la continuità temporale dello stesso;
- il rapporto “asimmetrico” tra il bullo e la vittima;
- l'anonimato e un senso di de-responsabilizzazione;
- l'assenza di limiti di spazio e di tempo e la facilità di accesso;
- un pubblico vasto e il rischio che il materiale diventi virale;
- la permanenza on line del materiale pubblicato;
- la rapida diffusione.

È possibile suddividere gli atti di cyberbullismo in due grandi categorie:

- cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei;

- cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima.

La mediazione tecnologica porta ad un certo distanziamento fra aggressore e vittima, causando quello che è stato definito come “disimpegno morale”. Si tratta di un indebolimento del controllo morale interno dell'individuo, con la conseguente convinzione di minimizzazione delle responsabilità individuali. Tale fenomeno vale non solo per il cyberbullo, ma anche per i cosiddetti “bystander”, ossia coloro che sono spettatori dei fatti. A ciò si aggiungono altre convinzioni o tendenze frequenti nell'uso della Rete, sia da parte dei giovani che degli adulti:

- la percezione che online non ci siano norme da rispettare;
- la sperimentazione online di identità e personalità multiple;
- il contesto virtuale come un luogo di simulazione e giochi di ruolo: i comportamenti messi in atto sono percepiti solo come un gioco;
- diffusione di responsabilità: tutti quelli che partecipano anche solo con un commento diventano, di fatto, corresponsabili.

L'Istituto Mattei, nella consapevolezza che le azioni efficaci siano quelle che ricorrono a strumenti educativi, rieducativi e di mediazione del conflitto, si impegna al tempo stesso a formare tutte le componenti della comunità scolastica in merito alle diverse responsabilità previste dalla normativa.

In primo luogo, si richiama l'art. 27 Cost. che stabilisce che la responsabilità penale è personale. Chi compie atti di bullismo e cyberbullismo può essere responsabile di reati e danni civili. Gli studenti che compiono azioni di bullismo e cyberbullismo possono commettere reati (percosse, lesioni personali, ingiuria, diffamazione, minacce, istigazione al suicidio ecc.). Si ricorda che per il nostro ordinamento l'imputabilità penale (ossia la responsabilità personale per i reati commessi) inizia dal quattordicesimo anno di età.

Le responsabilità per atti di bullismo e cyberbullismo compiuti dal minorenni possono ricadere anche su altri soggetti:

- i genitori, perché devono educare e vigilare su di loro, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando);
- gli insegnanti e la scuola (culpa in vigilando).
- esiste poi una “culpa in organizzando”, che si ha quando la scuola non mette in atto le azioni previste per la prevenzione dei comportamenti devianti o per affrontarli al meglio (così come previsto anche dalla normativa vigente).

In base a quanto previsto dalla Legge 71/2017 e le relative “Linee di orientamento per la prevenzione e il contrasto del cyberbullismo”, l'Istituto Mattei ha provveduto a individuare e a definire ruoli, responsabilità e azioni utili a prevenire e gestire i casi di bullismo e cyberbullismo. Tali azioni consistono in diverse tipologie di intervento:

- formazione del personale scolastico;
- formazione specifica del Dirigente scolastico e di alcuni docenti Referenti per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo);

- costituzione del Team per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo;
- sviluppo delle competenze digitali degli studenti, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti;
- previsione di misure di sostegno e rieducazione degli studenti coinvolti;
- integrazione del Regolamento d'Istituto e del Patto di corresponsabilità con specifici riferimenti a condotte di bullismo e cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- organizzazione di attività preventive ed educative e non solo sanzionatorie.

Per quanto riguarda le necessità di segnalazione e rimozione, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità sul 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 provvede, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore. Il Garante ha pubblicato sul proprio sito il modello per la segnalazione/reclamo in materia di cyberbullismo da inviare al seguente indirizzo mail: [cyberbullismo@gdpd.it](mailto:cyberbullismo@gdpd.it).

Parallelamente, nel caso in cui si ipotizzi che ci si possa trovare di fronte ad una fattispecie di reato, si può far riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo. È in tal senso possibile far riferimento a queste tipologie di uffici: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato on line (attraverso il portale <http://www.commissariatodips.it>).

Per un consiglio e un supporto è possibile rivolgersi alla Helpline di Telefono Azzurro per Generazioni Connesse: operatori esperti sono a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che degli studenti e dei genitori, che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative o problematiche inerenti l'utilizzo dei media digitali.

Sempre la Legge 71/2017 introduce un provvedimento di carattere amministrativo per gli autori di atti di cyberbullismo, la procedura di ammonizione da parte del Questore: il minore autore può essere convocato dal Questore e ammonito se ritenuto responsabile delle azioni telematiche. La procedura di ammonizione prevista in caso di condotte di stalking (art. 612-bis c.p.), in caso di condotte di ingiuria (art. 594 c.p.), diffamazione (art. 595 c.p.), minaccia (art. 612 c.p.) e trattamento illecito di dati personali (art. 167 del codice della privacy), commessi mediante Internet da minori ultraquattordicenni nei confronti di altro minore, se non è stata presentata querela o denuncia, è stata estesa al cyberbullismo. Gli effetti dell'ammonizione cessano al compimento della maggiore età.

---

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

Il fenomeno di "incitamento all'odio" o "discorso d'odio", comprende 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 è 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 coscienza consapevole e costruttiva da parte dei giovani.

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

Ogni istituzione scolastica deve attivarsi per garantire lo sviluppo di adeguate competenze digitali e per favorire un uso etico e consapevole delle nuove tecnologie. L’Istituto Mattei si impegna a fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, e promuove una partecipazione consapevole e costruttiva, anche attraverso i media digitali e i social network. Gli interventi di sensibilizzazione e prevenzione in tema di “hate speech” che la scuola organizza sono finalizzati al conseguimento di questi risultati:

- coinvolgere la comunità scolastica in percorsi di sensibilizzazione e di prevenzione dei comportamenti riconducibili all’hate speech;
- 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 l’elaborazione di un giudizio autonomo, consapevole e critico da parte degli studenti;
- coinvolgere le classi più problematiche, anche grazie all’intervento di esperti, come lo psicologo scolastico.

---

#### **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.

La dipendenza da Internet e il gioco online sono argomenti trasversali, che si affrontano nel corso delle attività di sensibilizzazione e prevenzione dedicate alla cittadinanza digitale, al cyberbullismo, all’uso consapevole dei dispositivi e della Rete.

L’Istituto Mattei organizza progetti e interventi specifici dedicati a stimolare negli studenti una riflessione sul fatto che la tecnologia deve essere uno strumento per raggiungere i propri obiettivi, e non sia solo fonte di

distrazione o addirittura un ostacolo al processo di apprendimento. La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo positivo e funzionale. Solo attraverso il controllo della tecnologia, si può sfruttare tutto il suo potenziale. È importante, quindi, non condannare a priori la tecnologia o il gioco on line, ma è necessario stabilire chiare e semplici regole di utilizzo, anche a livello di classe. Una soluzione applicata all'interno della scuola è quella di stabilire regole comuni e stipulare con gli studenti una sorta di "Regolamento di classe". Inoltre si propongono diverse metodologie didattiche che utilizzano come strumento i giochi virtuali d'aula (ad esempio adoperando il monitor interattivo di classe o il dispositivo personale). Allo stesso modo, quando si parla di videogiochi, è necessario concepirli non in termini negativi, ma di benessere digitale. Sono parte del mondo di studenti e studentesse.

---

#### **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.

Il sexting (abbreviazione di sex – sesso e texting – messaggiare, inviare messaggi) quindi, si configura con l'invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri. Tali contenuti sono realizzati con i dispositivi digitali, e sono diffusi in Rete e spesso diventano virali. Infatti, tali immagini o video, anche se inviati ad una stretta cerchia di persone, spesso si diffondono in modo incontrollabile e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che ritraggono minorenni al di sotto dei 18 anni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Inoltre i contenuti sessualmente espliciti possono diventare materiale di ricatto assumendo la forma del "revenge porn" (letteralmente "vendetta porno"). Tale fenomeno consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali con l'obiettivo di umiliare o ricattare la vittima (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di "revenge porn", con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Si veda l'articolo 612 ter del codice penale rubricato "Diffusione illecita di immagini o video sessualmente espliciti"). I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo, ansia e depressione.

Tra le attività che l'Istituto Mattei organizza al fine di contrastare tali fenomeni illeciti, vi sono:

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, anche condividendo diversi materiali, tra cui quelli messi a disposizione sul sito del progetto "Generazioni connesse";
- seguire gli alunni nella navigazione in Rete mentre svolgono le attività scolastiche e controllare periodicamente i siti visitati dagli alunni sui dispositivi scolastici;
- far rispettare il divieto di utilizzo di dispositivi digitali propri in orario scolastico, tranne nel caso della metodologia BYOD;
- approfondire in classe con attività mirate, la conoscenza dei

- rischi derivanti dall'uso scorretto dei dispositivi tecnologici;
  - predisporre apposite procedure di segnalazione e di contrasto dei comportamenti devianti;
  - partecipare agli eventi organizzati dai soggetti esterni in materia di sicurezza on-line.
- 

#### **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 ecc.), 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 gli interventi che l’Istituto Mattei organizza per prevenire ed affrontare la delicata problematica dell’adescamento.

Nella Convenzione il reato di adescamento viene definito come “qualsiasi atto volto a carpire la fiducia di un minore di anni 16 per scopi sessuali, attraverso artifici, lusinghe o minacce posti in essere anche mediante Internet o altre reti o mezzi di comunicazione”. Si parla di reato anche se l’incontro reale con il minore non avviene; è sufficiente, infatti, il tentativo.

Queste sono le fasi dell’adescamento on line:

- 1 – Fase dell’amicizia. L’adescatore instaura l’avvicinamento e crea il contatto con la vittima.
- 2 – Consolidamento del rapporto. Si rafforza l’amicizia e si instaura un clima di fiducia.
- 3 – Valutazione del rischio. Si controlla che non ci sia l’interferenza dei genitori o di altre persone adulte e si fa l’analisi degli aspetti logistici (descrizione dell’ambiente della vittima, dove è posizionato il PC, presenza o meno di adulti, ecc.).
- 4 – Fase di esclusività del rapporto. Si cerca di costruire un legame affettivo con la vittima e si instaura una profonda intimità virtuale.
- 5 – Fase sessuale. Si passa all’invio di materiale pornografico o all’incontro.

L’Istituto Mattei organizza percorsi di educazione (anche digitale) all’affettività e alla sessualità, in collaborazione con esperti interni (Sportello di ascolto psicologico) ed esterni. Ciò contribuisce a rendere gli studenti 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. Gli adulti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi del digitale, dell’affettività e della sessualità.

#### **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 Mattei organizza periodicamente attività ed interventi di sensibilizzazione e formazione, al fine di prevenire i fenomeni di pedopornografia, anche con la collaborazione di esperti interni (psicologo scolastico) e di soggetti esterni (Polizia postale). Gli studenti acquisiscono in questo modo quelle competenze in grado di orientarli e guidarli nelle loro scelte anche online; per questo motivo, l’educazione, compresa l’educazione all’affettività, riveste un ruolo fondamentale. In un’ottica di prevenzione, il tema della pedopornografia, anche se delicato, deve essere trattato a scuola, modulando gli interventi in base alla maturità e alla fascia di età degli studenti e selezionando il tipo di informazioni che si possono condividere. Risulta quindi utilissima l’attività educativa sull’affettività e sulle relazioni in generale: docenti e genitori devono porsi come figure di aiuto e supporto. Tutti gli studenti della scuola studiano materie giuridiche, e quindi apprendono le nozioni fondamentali sul diritto all’immagine e sulle

responsabilità penali e civili. La pedopornografia è 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, rientra nelle tematiche trattate nelle attività di sensibilizzazione e formazione rivolte al personale scolastico e ai genitori.

### ***Il nostro Piano d'azioni***

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

- 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.
- 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 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.

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

- 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.

## 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 potranno 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 e del 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, ecc.).

Nell'affrontare i casi è possibile che si coinvolgano 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 dalle 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 i Consigli di classe che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, attraverso comunicazioni pubblicate sul sito della scuola, 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 alla vittima? ecc.). 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; 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. Si ricorda che la normativa in vigore prevede che la persona coinvolta in qualità di vittima o testimone di 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 on line 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, e il blocco della sua diffusione.

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.

Si possono utilizzare, 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.

Ogni persona che venga a conoscenza o che abbia il sospetto di comportamenti illeciti è tenuta a segnalarlo ad uno dei seguenti soggetti: Coordinatore di classe, Dirigente scolastico, Referenti per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo. E' necessario assicurare la riservatezza delle informazioni.

Nella segnalazione è necessario indicare:

- le persone coinvolte (responsabili dell'episodio, vittime, altre persone coinvolte: sostenitori, spettatori passivi, ecc.);
- eventuali testimoni che abbiano assistito all'episodio;
- un resoconto quanto più circostanziato dei fatti;
- ogni altro elemento utile a ricostruire l'accaduto (materiale on line, altri documenti, testimonianze, note disciplinari, precedenti provvedimenti disciplinari ecc.).

Eventuali testimoni che vogliano rilasciare dichiarazioni, ma non vogliono che il loro nominativo sia comunicato all'alunno coinvolto, possono essere sentiti in separata sede (deve essere presente il Coordinatore e un altro docente che verbalizza le dichiarazioni).

La segnalazione deve essere tempestiva. Questo permette di:

- fornire alla vittima il supporto necessario;
- ricostruire la dinamica dei fatti;
- evitare la reiterazione di eventuali condotte scorrette;
- evitare che si commettano infrazioni più gravi;
- organizzare gli opportuni interventi di prevenzione e di contrasto dei fenomeni illeciti;
- coinvolgere eventuali soggetti esterni.

## **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 presentare due situazioni:

- 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.

---

### **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.

Per aiutare gli studenti a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, l'Istituto Mattei ha previsto specifiche procedure di segnalazione:

- segnalazione della situazione al docente Coordinatore di classe o ad un docente del Consiglio di classe;
- consulenza presso lo Sportello di ascolto psicologico (psicologo scolastico);
- segnalazione al Dirigente scolastico;
- segnalazione ai Referenti per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo.

L'insegnante di una scuola pubblica è un pubblico ufficiale anche fuori dall'orario scolastico; il collaboratore scolastico è un incaricato di un pubblico servizio, sul quale comunque incombono precisi obblighi di vigilanza. La conseguenza è che tali soggettività hanno l'obbligo di segnalare eventuali comportamenti illeciti al Dirigente scolastico o di denunciare, alle autorità competenti, i fatti di cui siano venuti a conoscenza e che costituiscono "reati" procedibili d'ufficio (es. violenza privata, estorsione, e via di seguito). Ai sensi

del comma 1 dell'art. 5 della Legge n.71 del 2017, salvo che il fatto costituisca reato, 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.

I docenti possono utilizzare la Scheda di segnalazione allegata.

Al fine di prevenire e contrastare i fenomeni di bullismo e cyberbullismo e di monitorare eventuali situazioni a rischio o sospette, i docenti possono compilare il Diario di bordo allegato.

### **PROCEDURA CONSIGLIATA IN CASO DI SOSPETTO DI FENOMENI DI BULLISMO O CYBERBULLISMO**

Il docente sospetta che stia accadendo qualcosa tra gli studenti della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo. Si consiglia di seguire la seguente procedura:

- confrontarsi con i Referenti per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo (Team antibullismo): valutare con loro le possibili strategie di intervento;
- confrontarsi con il Coordinatore di classe e valutare se è il caso di coinvolgere il Consiglio di classe;
- valutare se è il caso di avvisare il Dirigente Scolastico, anche in base al Regolamento d'Istituto.

Interventi sulla classe:

- organizzare con il Consiglio di classe attività finalizzate alla formazione degli studenti e alla prevenzione dei fenomeni devianti;
- coinvolgere lo psicologo scolastico nelle attività organizzate per la classe e ricordare agli studenti che possono anche usufruire individualmente dello Sportello psicologico;
- valutare il clima di classe, ascoltando i ragazzi e monitorando ciò che accade (ma senza fare indagini o interrogatori);
- valutare il grado di diffusione del fenomeno a livello di classe;
- parlare in classe del bullismo e del cyberbullismo e delle possibili conseguenze (non nominare gli alunni che si sospettano coinvolti). Informare gli studenti su quello che prevede la legge italiana su cyberbullismo (L. 71/2017);
- organizzare attività sull'empatia e sul riconoscimento delle emozioni (proprie e altrui).

Se emergono evidenze passare al punto successivo;

- ricordare agli studenti che possono segnalare al gestore del sito o del social e al Garante della privacy eventuali contenuti offensivi o lesivi che li riguardano;
- se, come docente, si ha un dubbio su come procedere o interpretare quello che sta accadendo, si può chiedere, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.
- ricordare agli studenti che possono chiedere una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat.

## **PROCEDURA CONSIGLIATA IN CASO DI EVIDENZA DI BULLISMO, CYBERBULLISMO, SEXTING, REVENGE PORN, ADESCAMENTO ON LINE**

Il docente ha evidenza che stia accadendo qualcosa tra gli studenti della propria classe, riferibile a un episodio di bullismo, cyberbullismo, sexting, revenge porn, adescamento on line, ecc. Si consiglia di seguire la seguente procedura:

- il docente compila la Scheda di segnalazione (vedi allegato – non è necessario compilare tutti i campi) e avvisa immediatamente il Dirigente scolastico, il Coordinatore di classe, i Referenti per il cyberbullismo e i membri del Team antibullismo;
- il Dirigente scolastico, insieme al Team antibullismo, al Coordinatore di classe e al docente coinvolto, individua le strategie opportune da intraprendere, in base alla gravità dell'episodio;
- il Coordinatore di classe e il docente coinvolto compilano e aggiornano il Diario di bordo (vedi allegato), in modo da monitorare la situazione e registrare le azioni intraprese.

### Non sono stati commessi reati e i comportamenti non sono di particolare gravità

- Valutare se è il caso di convocare un Consiglio straordinario per adottare eventuali provvedimenti disciplinari.
- Coinvolgere lo psicologo scolastico nelle attività organizzate per la classe e ricordare agli studenti che possono anche usufruire individualmente dello Sportello psicologico.
- Salvo che il fatto costituisca reato, il Dirigente scolastico, qualora venga a conoscenza di atti di bullismo e cyberbullismo, deve informare tempestivamente i genitori dei minori coinvolti. Valutare l'ipotesi di coinvolgere lo psicologo scolastico.
- Informare i genitori 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).
- Se si hanno dubbi su come procedere o interpretare quello che sta accadendo, si può chiedere una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

### Interventi sulla classe

- Cercare di capire il livello di diffusione del fenomeno.
- Organizzare attività di sensibilizzazione sul bullismo e il cyberbullismo (non nominare gli alunni coinvolti). Organizzare attività laboratoriali in modo da facilitare l'elaborazione e la comprensione di quanto accaduto.
- Supportare la vittima e responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.
- Coinvolgere lo psicologo scolastico nelle attività organizzate per la classe e ricordare agli studenti che possono anche usufruire individualmente dello Sportello psicologico.

### Sono stati commessi reati e i comportamenti sono di particolare gravità

- I minori che hanno compiuto 14 anni, vittime del reato, e i genitori o chi esercita la responsabilità genitoriale, possono presentare querela nei confronti degli autori del reato.
- Rivolgersi alla Polizia Postale e delle telecomunicazioni

affinché si rintraccino e si blocchino i responsabili. A seconda della situazione e delle valutazioni effettuate con Dirigente scolastico, Referente e genitori, si potrebbe poi segnalare alla Polizia Postale:

1. contenuto del materiale online offensivo;
  2. modalità di diffusione;
  3. fattispecie di reato eventuale.
- Tenere traccia di quanto accaduto e delle azioni intraprese: il Coordinatore di classe e il docente coinvolto compilano e aggiornano il Diario di bordo (vedi allegato).
  - Se è opportuno, richiedere un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).
  - Per qualsiasi dubbio, chiedere un consiglio telefonico alla helpline del progetto Generazioni Connesse al numero gratuito 1.96.96. Se i contenuti sono online segnala ai servizi di Generazioni Connesse “clicca e segnala” o “stop it”.

#### Interventi sulla classe

- Cercare di capire il livello di diffusione del fenomeno e parlare della necessità di non diffondere ulteriormente online i materiali.
- Parlare del bullismo, del cyberbullismo, del sexting, del revenge porn e dell'adescamento on line e delle possibili conseguenze (non nominare gli alunni coinvolti). Organizzare attività laboratoriali in modo da facilitare l'elaborazione e la comprensione di quanto accaduto.
- Supportare la vittima e responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.
- Parlare della necessità di non divulgare i materiali online e dei pericoli connessi ad una diffusione incontrollata.
- Informare gli studenti su ciò che prevede la normativa sul sexting, sulla diffusione di materiale pedopornografico e sull'adescamento online (L. 172/2012).
- Coinvolgere il Consiglio di classe e lo psicologo scolastico per organizzare percorsi di prevenzione dei comportamenti a rischio.
- Proporre la realizzazione di percorsi di sensibilizzazione e prevenzione dedicati a:
  1. Educazione all'affettività e alla sessualità (anche online)
  2. Immagine di sé online
  3. Relazioni interpersonali e online

In caso di convocazione del Consiglio di classe, è necessario fare riferimento alla procedura prevista dal Regolamento d'Istituto.

---

### **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 dalle possibilità della scuola.

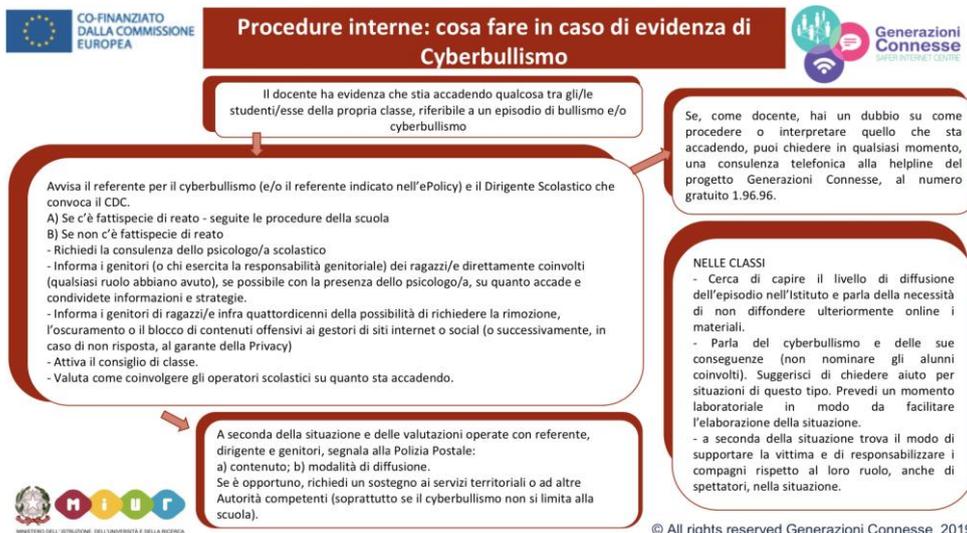
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse “Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani” (seconda parte, pag. 31), senza

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.

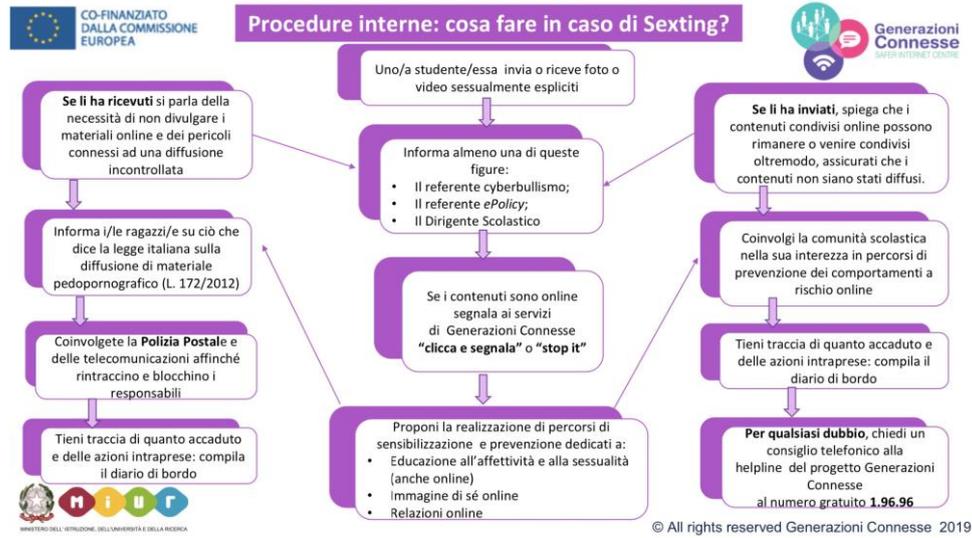
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute 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.

## 5.4. - Allegati con le procedure

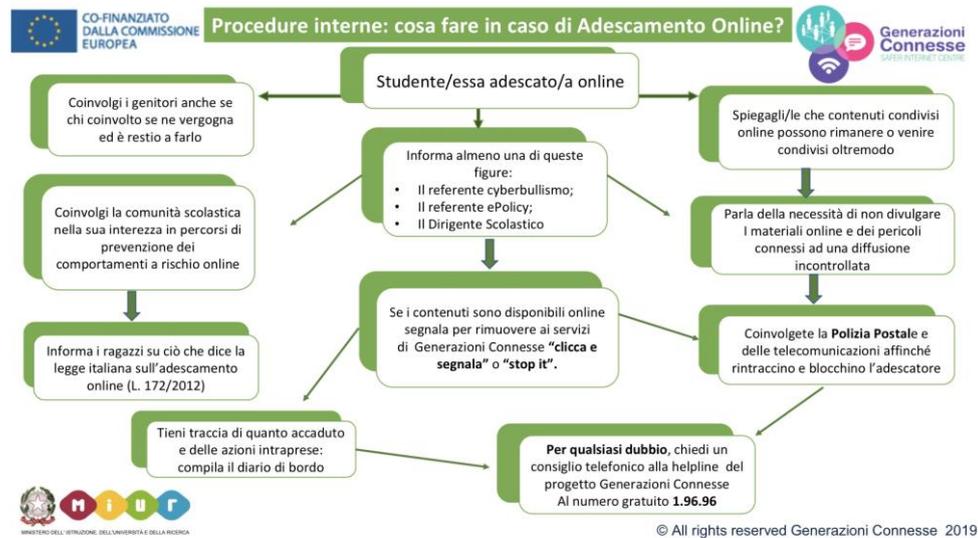
### Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



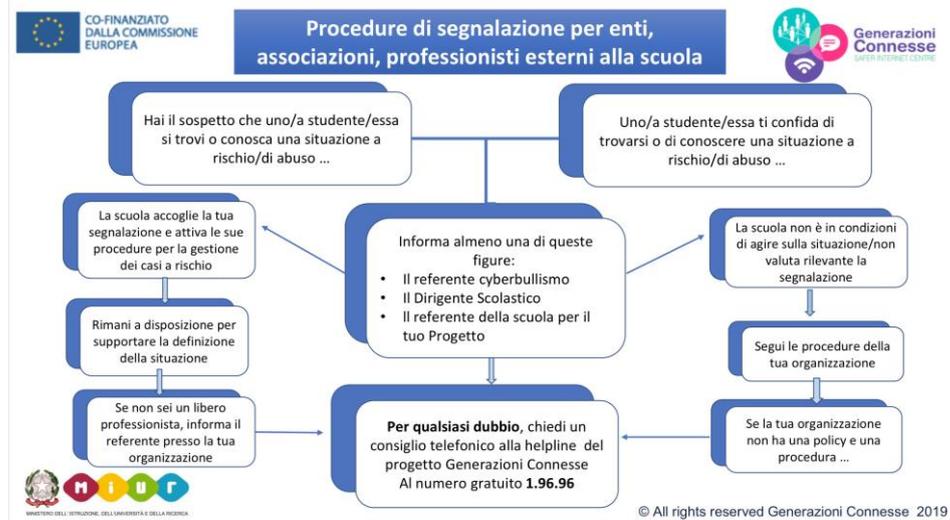
## Procedure interne: cosa fare in caso di sexting?



## 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 dei reati procedibili d'ufficio

## Il nostro Piano d'azioni

- Condividere con tutte le componenti scolastiche il documento di ePolicy.
- Integrare il documento di ePolicy con il Regolamento d'Istituto.
- Organizzare attività di sensibilizzazione, formazione, prevenzione e contrasto dei comportamenti devianti, destinate agli studenti, al personale scolastico e ai genitori.
- Collaborare con gli attori presenti sul territorio:
  - altre istituzioni scolastiche e Rete Ri-connect;
  - esperti interni (Psicologo scolastico) ed esterni (professionisti, Università, ecc.);
  - Forze dell'ordine.