



Documento di ePolicy

AQMM060003

IST. ONNICOMPENSIVO A. ARGOLI

VIA G. MARCONI N.51 - 67069 - TAGLIACOZZO - L'AQUILA (AQ)

Clementina Cervale

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- 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 rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento

1. **Presentazione dell'ePolicy**

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

2. **Formazione e curriculum**

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

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

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

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

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

5. **Segnalazione e gestione dei casi**

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

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

Attraverso l'E-policy l'Istituto Onnicomprensivo Argoli di Tagliacozzo (Aq) vuole dotarsi di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento al fine di garantire un approccio alla tecnologia che sia consapevole, critico ed efficace nonché sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet. L'obiettivo è quello di essere pronti a cogliere i cambiamenti in atto nell'attuale società in particolare per quanto riguarda la formazione dei cittadini del futuro, destinati a vivere in un ambiente in cui tutto, oramai, viene gestito attraverso l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC). Le tecnologie diventano quotidiane, ordinarie, al servizio dell'intera comunità educante. Con questo documento si vuole quindi, regolamentarne l'uso per rendere responsabili tutti gli utenti dell'Istituto senza trascurare la tutela della privacy. Le indicazioni nazionali invitano a potenziare le competenze digitali degli studenti, ai quali è richiesto di sapersi orientare nelle molteplici possibilità offerte dal Web, analizzando criticamente i materiali disponibili, scambiando informazioni ed esperienze in modo consapevole e responsabile. L'Istituto Onnicomprensivo Argoli è una scuola che ha potenziato, nel corso degli anni, la propria dotazione tecnologica arredando tutte le classi con LIM o schermi interattivi; la scuola è inoltre aperta all'uso del BYOD e possiede una discreta dotazione di device portatili e che permettono la realizzazione di attività didattiche su piattaforma educative telematiche.. Anche per questo, negli ultimi anni, a fronte del varo del Piano Nazionale della Scuola Digitale l'Istituto ha riservato particolare attenzione alla formazione del personale attivando o promuovendo corsi per l'acquisizione di competenze digitali, l'integrazione delle TIC nella Didattica, l'utilizzo della piattaforma educativa G-Suite for Education. Ad oggi la G-Suite for Education è correntemente utilizzata dalla totalità dei docenti sia per le attività di DDI che per frequentare i corsi di formazione erogati dal team digitale. La scuola ha inoltre ottenuto, per il biennio 2020-2021, il label di scuola eTwinning. Questi motivi, a fronte, anche, del recente lock-down che ha reso capillare, prima con la Didattica a Distanza e poi con la Didattica Digitale Integrata, l'utilizzo delle TIC, hanno reso necessario l'elaborazione di un efficace strumento di e-Policy. Gli obiettivi che ci proponiamo con questo documento sono, prima di tutto, di regolamentare l'utilizzo delle tecnologie digitali affinché gli studenti e le studentesse ne dispongano in maniera positiva, critica e consapevole; e in secondo luogo, di formare i docenti, e la comunità educanda tutta, per accrescere e consolidare le competenze di cittadinanza digitale oltre ad un uso sicuro e creativo della rete e delle sue risorse.

1.2 - Ruoli e responsabilità

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

Il nostro documento è stato elaborato in armonia con il Patto di corresponsabilità e gestione cyberbullismo, affinché sia realmente uno strumento operativo efficace per la nostra scuola e che tutta la comunità educante, ciascuna nel proprio ruolo, s'impegni nell'attuazione e promozione delle regole e delle pratiche ivi contenute

LA DIRIGENTE SCOLASTICA:

La Dirigente Scolastica, prof.ssa Clementina Cervale, garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. Promuove la cultura della sicurezza online e dà il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. La medesima DS ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'ANIMATORE DIGITALE:

L'Animatore digitale, prof.ssa Margherita Del Manso, supporta il personale scolastico da un punto di vista non solo tecnico- informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre 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 fornisce agli utenti autorizzati della scuola apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

IL REFERENTE BULLISMO E CYBERBULLISMO

"Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo". Il referente del Bullismo e Cyberbullismo, prof.ssa Antonella Finucci, ha il compito di coordinare e promuovere iniziative specifiche di prevenzione e contrasto. A tal fine, può avvalersi della collaborazione delle Forze dell'Ordine, delle Associazioni e dei Centri di aggregazione giovanile presenti sul territorio

I DOCENTI

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Promuovono, laddove possibile, l'uso delle tecnologie digitali nella didattica, accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi

tecnologici che si connettono alla Rete; hanno il dovere morale e professionale di segnalare alla Dirigente Scolastica qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

IL PERSONALE AMMINISTRATIVO TECNICO E AUSILIARIO

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 La Dirigente Scolastica e con il personale docente tutto. Il personale ATA è altresì coinvolto, all'interno dei singoli regolamenti d'Istituto, nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

GLI STUDENTI E LE STUDENTESSE

Gli Studenti e le Studentesse, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzano al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola imparano a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le; 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.

I GENITORI

I Genitori, in continuità con l'Istituto scolastico, potranno essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; potranno relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non utilizzano responsabilmente le tecnologie digitali o Internet. È estremamente importante che accettino e condividano quanto scritto nell'e-Policy dell'Istituto.

I SOGGETTI ESTERNI

Tutti gli enti educativi esterni e le associazioni che entreranno in relazione con la scuola si conformeranno alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC al fine di promuovere comportamenti sicuri, coadiuvare la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme. Il presente documento ricorda la corresponsabilità educativa e formativa coinvolge sia i genitori che la scuola. In particolare, il 2° 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, si richiama il 1° comma dell'art. 30 della Costituzione *"è dovere e diritto dei genitori mantenere, istruire ed educare i figli, anche se nati fuori del matrimonio"*; nonché il 1° 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 (...); e l'art. 147 del c.c. "l'obbligo di mantenere, istruire, educare e assistere moralmente i figli, nel rispetto delle loro capacità, inclinazioni naturali e aspirazioni (...)".

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

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

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

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

Tutti gli attori che avranno una relazione educativa con gli studenti e le studentesse dovranno mantenere costantemente un elevato profilo personale e professionale, eliminando condotte non professionali ed essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori. Sono vietati i comportamenti offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse. E' inoltre vietato tollerare o partecipare a comportamenti illegali abusivi da parte degli studenti possano mettere a rischio la loro sicurezza. Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole dell'Istituto Argoli dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, ecc.) e quelli in

dotazione della scuola, evitando un uso improprio o comunque deontologicamente inadeguato durante le attività con gli studenti e le studentesse. E' obbligatorio rispettare la privacy, soprattutto dei soggetti minorenni, riguardo a fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network). L'Istituto inoltre, in virtù del rapporto fiduciario esistente con le famiglie e in un'ottica di gestione condivisa degli interventi, segnalerà anche alle autorità competenti situazioni a rischio. L'Istituto si riserva il diritto di richiedere agli attori esterni il certificato del casellario giudiziale a ulteriore garanzia dei minori con l'obiettivo di verificare l'esistenza (o meno) di condanne per i reati previsti dal Codice penale e rubricati negli 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, ecc.) è un fattore preferenziale. È importante garantire che tutti i soggetti esterni che erogano attività in ambito scolastico siano sensibilizzati e resi consapevoli dei rischi online che possono correre gli studenti e le studentesse; dei comportamenti corretti che devono adottare a scuola se si ha il sospetto che uno studente si trovi o conosca una situazione a rischio e/o abuso. Il personale degli enti esterni può utilizzare i propri dispositivi personali (smartphone, tablet, pc, ecc.) ed eventualmente quelli in dotazione della scuola, evitando un uso improprio durante le attività con gli studenti e le studentesse, nel rispetto della normativa (Decreto legislativo 196 del 30 giugno 2003 mod. e int. Dal d lgs 101/2018 e Reg.to UE 2016/679).

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

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

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

- la pubblicazione del documento sul sito istituzionale della scuola;

- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

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

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

Il documento di E-policy, approvato dal Collegio dei docenti, viene condiviso con tutta la comunità educante, studenti, studentesse, personale docente e non, in conformità a quanto previsto dal codice di comportamento dei dipendenti pubblici, 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.

Gli studenti e le studentesse vengono altresì informati che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete anche al fine di far loro conoscere e prevenire comportamenti a rischio

1.5 - Gestione delle infrazioni alla ePolicy

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

L'Istituto gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, valutando la gravità delle eventuali violazioni anche in base ai diversi ordini di scuola. I provvedimenti disciplinari avranno finalità educativa e tenderanno al rafforzamento del senso di responsabilità degli alunni/e. Le eventuali infrazioni delle e-Policy verranno gestite dal Consiglio di Classe previa convocazione da parte della D.S. , secondo le modalità deliberate dal Collegio dei Docenti; per le violazioni, si procederà con un'ammonizione, una nota o sospensione disciplinare e la sanzione dell'allontanamento dalla comunità scolastica per i casi particolarmente gravi. Per l'individuazione dei comportamenti inadeguati e delle sanzioni previste, si rimanda al Regolamento di Istituto.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Il Regolamento dell'Istituto Scolastico verrà 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 che verranno emanate. Il presente documento sarà pubblicato, contestualmente al Regolamento di Istituto, su sito della scuola, sezione "Regolamenti".

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

L'E-policy verrà aggiornata periodicamente e/o quando si verificheranno cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno dell'Istituto. 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. A questo scopo la commissione della e-policy predisporrà un questionario di valutazione per stabilire limiti e punti di forza del piano di formazione approntato e dei percorsi educativi e didattici di prevenzione e gestione rischi.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

Azioni da svolgere nei prossimi 3 anni:

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

rivolto agli studenti

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

Capitolo 2 - Formazione e curriculum

2.1. Curriculum sulle competenze digitali per gli studenti

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

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

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

Il nostro Istituto è un onnicomprensivo, pertanto si dovrà prevedere un curriculum sulle competenze digitali che interessi gli alunni dalla scuola dell’Infanzia alla Sc.Sec.II Grado. A questo proposito la Scuola nel promuovere tali competenze ha la fortuna di essere in possesso di una buona attrezzatura elettronica che permette utilizzo di app che agevolano la lezione dell’insegnante e permettono di mettere in campo strategie formative valide. Si svilupperanno le seguenti aree: Area 1: “Alfabetizzazione e dati” con una dimensione “informazionale” o “cognitiva” delle competenze digitali. Essa è relativa alla capacità di cercare, selezionare, valutare e riprocessare le informazioni in Rete, puntando 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 (app, giochi online, siti non adatti ai minori). Area 2: “Comunicazione e collaborazione” Si farà riferimento a quelle competenze volte a riconoscere le giuste ed appropriate modalità per comunicare e relazionarsi online:

saper interagire con gli altri attraverso le tecnologie digitali; essere consapevoli nella condivisione delle informazioni in Rete; essere buoni “cittadini digitali”; collaborare adeguatamente con gli altri attraverso le tecnologie digitali; conoscere le “Netiquette”; Saper gestire la propria “identità digitale”. Area 3: “Creazione di contenuti digitali” Quest’area fa riferimento alle capacità di “valutare le modalità più appropriate per modificare, affinare, migliorare e integrare nuovi contenuti e informazioni specifici per crearne di nuovi e originali” (v. DigComp 2.1 “Quadro di riferimento per le competenze digitali dei cittadini”). Le specifiche competenze digitali che andranno sviluppate in questo caso sono: 1. Creare e modificare contenuti digitali in diversi formati per esprimersi attraverso mezzi digitali; 2. Modificare, affinare, migliorare e integrare informazioni e contenuti all’interno di un corpus di conoscenze esistente per creare conoscenze e contenuti nuovi, originali e rilevanti; 3. Capire come il copyright e le licenze si applicano ai dati, alle informazioni e ai contenuti digitali. Area 4: “Sicurezza” Quest’area è parte di una dimensione più generale definita come “benessere digitale” che include la necessità di salvaguardare i propri dati personali e rispettare le regole nel trattare i dati altrui. Nello specifico, bisognerebbe puntare a sviluppare negli studenti ad 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; 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 tutti siano formati ed aggiornati sull’uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

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

Le TIC dovrebbero essere usate dagli insegnanti ad integrazione della didattica al fine

di progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli studenti della classe, anche delle persone con disabilità (in chiave inclusiva). Di conseguenza, gli insegnanti dovrebbero avere o raggiungere un buon livello di formazione in merito all'utilizzo e l'integrazione delle TIC nella didattica, partendo da compiti semplici (individuare i fabbisogni informativi; trovare dati, informazioni e contenuti attraverso una semplice ricerca in ambienti digitali) per arrivare a compiti più complessi (ricercare e filtrare portali e offerte). Su tali premesse 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), sia dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online), purché restino coerenti con il piano di formazione.

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

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

L'Istituto si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti. Formare i docenti sulle tematiche in oggetto vuol dire non pensare esclusivamente all'alfabetizzazione ai media ma anche considerare la sfera emotiva e affettiva degli studenti 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 poter educare ragazzi e ragazze alle emozioni in contesto onlife e quindi modulare e gestire i propri ed altrui comportamenti, favorendo e promuovendo forme di convivenza civile.

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

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

A tale proposito è importante informare i genitori sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli, in riferimento ai rischi connessi ad un uso distorto della Rete da parte degli studenti.

Si potrebbero elaborare regole sull'uso delle tecnologie digitali da parte dei genitori nelle comunicazioni con la scuola e con i docenti (es. mail, gruppo whatsapp, sito della scuola, ecc.) e informarli adeguatamente anche riguardo alle regole per gli studenti; fornire ai genitori consigli o linee guida sull'uso delle tecnologie digitali nella comunicazione con i figli e in generale in famiglia (ad es. a tal fine si potrà fare riferimento alla sezione dedicata ai genitori del sito www.generazioniconnesse.it

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dei tre

anni scolastici successivi)

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

(cfr. <http://www.garanteprivacy.it/scuola>).

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

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

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

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

ISTITUTO ONNICOMPRESIVO STATALE "A. ARGOLI"
SCUOLE INFANZIA - PRIMARIA- SECONDARIA DI 1° GRADO - ISTITUTO
TECNICO ECONOMICO INDIRIZZO:TURISMO

Via Guglielmo Marconi, 51 - **67069 TAGLIACOZZO** - C.F.
81006950661

Segreteria tel. 0863/610335 -

Sito web: istitutoargoli.edu.it - **E-mail:**
aqmm060003@istruzione.it -

Pec: aqmm060003@pec.istruzione.it

Informativa per il trattamento di dati personali (Regolamento Europeo n.2016/679)

Ai sensi dell'art.13 del Regolamento UE n.2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali L'Istituto Onnicomprensivo Statale "A. Argoli" - Via G.Marconi, 51 - 61069 Tagliacozzo (AQ) rappresentato dal Dirigente Scolastico Prof.ssa Clementina Cervale, si comunica agli esercenti la responsabilità genitoriale, agli studenti e alle studentesse, ai docenti e a tutto il personale scolastico in merito a quanto segue relativamente ai dati personali.

TITOLARE DEL TRATTAMENTO DEI DATI

Il Titolare del trattamento dei dati è l'Istituto Onnicomprensivo Statale "A. Argoli", con sede Via Guglielmo Marconi, 51 Tagliacozzo (AQ) tel.0863 610335 e-mail: aqmm060003@istruzione.it , nella persona della Dirigente Scolastica, legale rappresentante dell'istituto, Prof.ssa Clementina Cervale

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della Protezione dei dati è la società Microtech srl raggiungibile al seguente indirizzo: Viale Dante 140/b - 03043 Cassino (FR), Tel. 0776 26110- e-mail: microtche@webmicrotech.it .

BASE GIURIDICA E FINALITÀ DEL TRATTAMENTO

I dati personali forniti alla presente Istituzione scolastica, anche se raccolti presso il Ministero dell'Istruzione e le sue articolazioni periferiche, in fase di iscrizione e successivamente, saranno trattati dal personale della scuola soltanto nell'ambito delle finalità istituzionali, che sono quelle relative all'istruzione ed alla formazione degli alunni e quelle amministrative ad esse strumentali. Il trattamento dei dati sarà improntato ai principi di correttezza, liceità, trasparenza, limitazione delle finalità, esattezza, limitazione della conservazione, integrità e tutela della riservatezza e dei diritti individuali. I dati personali definiti come "categorie particolari di dati personali" o come "dati personali relativi a condanne penali e reati" dagli art. 9 e 10 del Regolamento Ue 2016/679, saranno trattati esclusivamente dal personale della scuola, appositamente incaricato, secondo quanto previsto dalle disposizioni di Legge e di Regolamento nel rispetto del principio di stretta indispensabilità dei trattamenti. La base giuridica del trattamento è l'esecuzione di un compito di interesse pubblico o connesso all'esercizio pubblici poteri da parte del Titolare derivante da normativa nazionale

LEGITTIMAZIONE E CONSENSO

Nel corso del rapporto con la presente Istituzione scolastica, i dati personali verranno trattati dal personale della scuola nell'ambito delle finalità istituzionali, così come definite dalla normativa vigente: R.D. n. 653/1925, D.Lgs n. 297/1994, D.P.R. n. 275/1999; D.I. n. 129/2018 e le norme in materia di contabilità generale dello Stato; L. n. 104/1992, L. n. 53/2003, D.Lgs n. 165/2001, D.Lgs 196/2003 e ss.mm.ii, Reg. Ue 2016/679 D.lg 10/08/2018 n. 101; D.M 305/2006; D.Lgs 76/05; D.Lgs 77/05; D.Lgs 226/05; D.Lgs n. 151/2001; D.P.C.M. n. 185/2006; D.P.R. n. 89/2009; L. 170/2010; D.M. n. 5669/2011; D.P.R. 80/2013, D. Lgs 33/2013, D.L. 104/2013, convertito, con modificazioni, dalla L. 128/2013, L. 107/2015, D. Lgs 50/2016 e ss.mm.ii., relativi decreti applicativi e tutta la normativa collegata alle citate disposizioni. Si fa presente che il conferimento dei dati richiesti e il conseguente trattamento sono obbligatori, in quanto previsti dalla normativa sopra citata; l'eventuale rifiuto a fornire tali dati potrebbe comportare il mancato perfezionamento dell'iscrizione e l'impossibilità di fornire all'alunno tutti i servizi necessari per garantire il suo diritto all'istruzione ed alla formazione. La presente Istituzione scolastica dovrà ottenere il consenso dell'interessato per raccogliere e trattare i dati relativamente ai trattamenti complementari alle finalità istituzionali.

MODALITÀ DI TRATTAMENTO

Il trattamento dei dati sarà effettuato sia con strumenti cartacei che

elettronici, nel rispetto delle misure di sicurezza minime, così come previsto dal Regolamento Europeo, ad opera di soggetti appositamente autorizzati al trattamento dei dati dall'Istituto scolastico. Sono autorizzati al trattamento dei dati: il personale amministrativo, tecnico e ausiliario in servizio presso l'Istituto; i docenti in servizio presso l'Istituto; eventuali docenti ed esperti esterni incaricati dalla scuola di svolgere attività di ampliamento dell'offerta formativa, come previsto dal PTOF. Il personale autorizzato ha accesso ai dati a seconda delle mansioni e si attiene alle norme impartite e alle disposizioni di legge. È vietato all'incaricato qualsiasi forma di diffusione e comunicazione di dati personali che non sia funzionale allo svolgimento dei compiti affidati e su cui non sia stato adeguatamente istruito per quanto riguarda la normativa in materia di privacy.

CHI HA ACCESSO AI DATI

Potranno accedere, e quindi venire a conoscenza dei dati personali, solo i soggetti autorizzati al trattamento quali gli addetti autorizzati dell'area amministrativa e didattica appositamente designati.

CONSERVAZIONE E TRATTAMENTO

I dati saranno conservati presso gli archivi del Titolare per tutta la durata del rapporto tra gli utenti e l'istituzione scolastica, per l'espletamento di tutti gli adempimenti di legge e per un tempo non superiore agli scopi per i quali sono stati raccolti. In ogni caso i dati sono conservati secondo le indicazioni delle Regole tecniche in materia di conservazione digitale degli atti definite da AGID e nei tempi e nei modi indicati dalle Linee Guida per le Istituzioni scolastiche e dai Piani di conservazione e scarto degli archivi scolastici definiti dalla Direzione Generale degli Archivi presso il Ministero dei Beni Culturali.

DESTINATARI DEI DATI

I dati personali potranno essere comunicati a soggetti pubblici (quali, ad esempio, ASL, Comune, Provincia, Ufficio Scolastico Regionale, Ambiti Territoriali, organi di Polizia Giudiziaria, organi di Polizia Tributaria, Guardia di Finanza, Magistratura) nei limiti di quanto previsto dalle vigenti disposizioni di Legge e di Regolamento e degli obblighi conseguenti per codesta Istituzione scolastica; i dati relativi agli esiti scolastici degli alunni potranno essere pubblicati mediante affissione all'albo della scuola secondo le vigenti disposizioni in materia. I dati forniti potranno essere comunicati altresì alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente alla carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio. Potranno

infine venire a conoscenza dei dati personali docenti ed esperti esterni incaricati dalla scuola a svolgere attività di ampliamento dell'offerta formativa, come previsto dal PTOF, nonché soggetti terzi che forniscono, a questa Istituzione scolastica, servizi strumentali (alle finalità di cui sopra), ferma restando la garanzia di tutela dei diritti dell'interessato. Tali soggetti agiranno in qualità di Responsabili o di Autorizzati al trattamento. La realizzazione di questi trattamenti costituisce una condizione necessaria affinché l'interessato possa usufruire dei relativi servizi. Ai sensi dell'art. 96 del D.LGS 196 del 2003, ferma restando la tutela della riservatezza dell'alunno, al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, i dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento, possono essere comunicati o diffusi, anche a privati e per via telematica dall'istituzione scolastica. La comunicazione o la diffusione avverrà su richiesta dell'interessato e i dati saranno poi trattati esclusivamente per le predette finalità. I dati particolari e quelli relativi a condanne penali o reati (artt. 9 e 10 GDPR) non saranno oggetto di diffusione; tuttavia, alcuni di essi potranno essere comunicati ad altri soggetti pubblici nella misura strettamente indispensabile per svolgere attività istituzionali previste dalle vigenti disposizioni di legge in materia sanitaria, previdenziale, tributaria, giudiziaria e di istruzione.

TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI

Non sono previsti trasferimenti di dati personali verso Paesi terzi (extra-UE) o organizzazioni internazionali.

DIRITTI

Al Titolare del trattamento l'interessato potrà rivolgersi, per far valere i propri diritti, così come previsto dagli articoli 15 e seguenti del Regolamento Europeo 2016/679; ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano. L'interessato ha i seguenti diritti:

- di accesso;
- di rettifica;

per i dati non obbligatori per le finalità istituzionali:

- di cancellazione (diritto all'oblio);
- di limitazione del trattamento;
- di opposizione;

- alla portabilità;
- di revoca del consenso, nei casi previsti dal Regolamento.

L'interessato potrà esercitare tutti i diritti di cui sopra inviando una e-mail al Responsabile della Protezione dei dati al seguente indirizzo: microtech@webmicrotech.it . L'interessato ha inoltre diritto di proporre reclamo all'Autorità di controllo dello Stato di residenza (Garante Privacy).

LA DIRIGENTE SCOLASTICA

Clementina Cervale

(Documento firmato digitalmente ai sensi del Codice dell'Amministrazione Digitale e normativa connessa)

3.2 - Accesso ad Internet

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

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure

riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

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

Condizioni Attuali: L'Istituto, in ogni suo plesso, è dotato di rete wi.fi, la sede centrale ha anche un accesso alla rete ADSL separato per gli usi di segreteria e per i laboratori, linguistico e informatico. Ogni aula della sede centrale è dotata di Dashboard e pc in modo da garantire ad ogni gruppo classe l'accesso ad internet e la possibilità per ogni docente di creare, usufruire e gestire contenuti multimediali. Nelle sedi della scuola primaria e dell'infanzia il numero di dashboard e pc è ridotto e sono disposte in aule comuni e utilizzate su richiesta dei docenti.

In seguito all'analisi dei bisogni di ogni plesso, l'istituto ha partecipato e ottenuto finanziamenti per implementare la strumentazione e la capacità della rete anche per la scuola primaria e dell'infanzia. Allo stato attuale le rete in dotazione non consente a tutti gli studenti di accedere, con proprio username e password, ad internet.

La scuola si è dotata inoltre dei seguenti regolamenti:

- Accesso ai laboratori informatico e linguistico
- Regolamento sull'uso consapevole della rete
- Regolamento per la didattica a distanza e per la DDI

Pubblicati sul sito d'Istituto - Sezione: Scuola - sotto sezione: le carte della scuola - Regolamenti

3.3 - Strumenti di comunicazione

online

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

L'uso degli strumenti di comunicazione online, affianco di quelli tradizionali, ha l'obbiettivo di rendere lo scambio comunicativo più interattivo.

Gli strumenti di comunicazione utilizzati dalla scuola curano sia la comunicazione interna che esterna.

Relativamente alla **comunicazione interna** la scuola si impegna ad un uso completo e continuativo del registro elettronico, tramite il quale i responsabili genitoriali e gli alunni possono verificare l'andamento scolastico (frequenza, voti, note disciplinari, comunicazioni e circolari) ed essere aggiornati su tutte le attività curriculari ed extracurriculari.

Per **comunicazione esterna** la scuola utilizza il sito web, il canale youtube, instagram e il profilo facebook; inoltre tutti gli utenti, docenti e studenti, tramite l'account personale, possono accedere alla piattaforma GSuite for education. Gli account vengono rimossi quando si interrompe il rapporto scolastico.

3.4 - Strumentazione personale

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

La presente **ePolicy** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e

riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

I dispositivi tecnologici sono oramai parte integrante della vita di ciascuno di noi compresa quella degli studenti e studentesse dei docenti che influenzano necessariamente la didattica e gli stili di apprendimento. E' pertanto fondamentale che la comunità scolastica adotti regole condivise sull'uso delle tecnologie considerando aspetti positivi e potenziali criticità. L'Istituto Argoli promuove e supporta l'uso dei dispositivi elettronici durante lo svolgimento dell'attività didattica purché l'utilizzo avvenga previa autorizzazione del docente e nel rispetto degli altri utenti e componenti della classe. L'eventuale uso scorretto degli stessi verrà sanzionato secondo quanto previsto dal regolamento di Istituto.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare 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

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

Scegliere almeno 1 di queste azioni:

- 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 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)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

- Nel caso della **sensibilizzazione** si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.
- Nel caso della **prevenzione** si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

CAPITOLO 4, 1: RISCHI ON LINE CONOSCERE PREVENIRE E RILEVARE

E' necessario che la scuola metta in atto un processo di sensibilizzazione all'utilizzo delle tecnologie digitali in rete, per prevenire i rischi di un uso inconsapevole e superficiale.

L'istituto onnicomprensivo A.Argoli di Tagliacozzo, intende perseguire azioni di prevenzione universale e di sensibilizzazione con l'autorizzazione delle famiglie e la collaborazione della rete di servizi territoriali, servizi sociali e Forze di polizia postale, atti a formare e consolidare competenze educative necessarie a poter gestire e arginare i rischi derivanti dalla navigazione in rete.

Gli strumenti indispensabili per poter ridurre tali rischi sono gli interventi di sensibilizzazione e prevenzione.

Sensibilizzazione attraverso azioni utili a far conoscere il fenomeno anche attraverso video e materiale illustrativo- brochure, per poter comprendere i comportamenti da adottare.

Prevenire attraverso attività, azioni, interventi atti a promuovere competenze digitali tali da far riconoscere ed evitare l'insorgenza dei rischi legati alla rete.

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).

CAPITOLO 4, 2 CYBERBULLISMO, CHE COSA E' E COME PREVENIRLO

Il cyberbullismo è la manifestazione in rete del fenomeno del bullismo perpetrato in rete attraverso i social network, con la diffusione di messaggi denigratori, foto e immagini offensive o tramite la formazione di gruppi contro una presunta vittima.

Il nostro ordinamento giuridico fino a poco tempo fa non contemplava una definizione di Cyberbullismo, ma con **la legge del 29 maggio del 2017 n°71** riguardante le "disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo.", il fenomeno è stato isolato. **Nell'articolo 1 comma 2** con il termine cyberbullismo si intende qualunque forma di aggressione, pressione, molestia, ricatto, denigrazione, furto d'identità, alterazione, diffamazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali a danno dei minorenni, realizzata per via telematica, nonché la diffusione dei contenuti on -line aventi ad oggetto anche uno o più componenti della famiglia del minore o 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 referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali , tra gli obiettivi formativi prioritari l. 107 del 2015:
- promozione di un ruolo attivo degli studenti in attività di peer to peer;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti e 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 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 **azione di supporto al DIRIGENTE SCOLASTICO** per la revisione e la stesura dei regolamenti atti e documenti PTOF, PDM, RAV.

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

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

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

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

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

CAPITOLO 4, 3 - HATE SPEECH:CHE COS'E' E COME PREVENIRLO.

Il fenomeno di incitamento all'odio o discorso d'odio , indica discorsi e

pratiche che esprimono odio e intolleranza verso un gruppo o una persona e che rischiano di provocare reazioni violente a catena. nello specifico con il termine "HATE SPEECH" si indica un'offesa fondata su una qualsiasi discriminazione, razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, ai danni di una persona o di un gruppo.

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

fornire agli studenti gli strumenti necessari per decostrire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;

promuovere la partecipazione civica e l'impegno anche attraverso i media digitali e i social network;

favorire una presa di parola consapevole e costruttiva da parte dei giovani.

4.4 - Dipendenza da Internet e gioco online

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

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

CAPITOLO 4, 4 - DIPENDENZA DA INTERNET E GIOCO ONLINE

Il benessere digitale è fondamentale per le giovani generazioni, poiché un uso incontrollato ed eccessivo, genera dipendenza e crea effetti negativi sullo sviluppo evolutivo e sulle relazioni sociali.

L'Istituto onnicomprensivo A.Argoli vuole promuovere la capacità di creare e mantenere una relazione sana con la tecnologia, usare la tecnologia per raggiungere obiettivi e non come distrazione oppure ostacolo, controllare la tecnologia e usarne le potenzialità e vantaggi. Inoltre si terranno in considerazione due aspetti fondamentali: **la consapevolezza dello status quo e la motivazione al cambiamento**, fornendo informazioni chiare sulle tematiche dell'uso consapevole della rete.

I percorsi sul benessere digitale si attiveranno attraverso azioni come:

call to action di telefono azzurro, grazie al protocollo di intesa stipulato da telefono azzurro con il ministero dell'istruzione per la promozione di azioni di educazione alla cittadinanza digitale nelle scuole, nell'ambito del piano nazionale per la scuola digitale.

Promuovere incontri e laboratori per studenti e studentesse dedicati all'educazione digitale

organizzare laboratori e realizzare progetti di peer to peer education sui temi dell'uso di internet e sui rischi delle tecnologie digitali

organizzare incontri di sensibilizzazione per la prevenzione dei rischi con le famiglie.

Il referente e il gruppo di lavoro costituito dai docenti della scuola primaria e secondaria, in accordo con il team digitale e l'animatore digitale si adopereranno per la segnalazione e il monitoraggio degli episodi e attori coinvolti.

L'istituto è intenzionato , nel prossimo triennio a promuovere azioni e progetti di prevenzione attraverso percorsi sul benessere digitale.

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 mediali 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.

CAPITOLO 4. 5 SEXTING

Il sexting è tra i rischi più diffusi connessi ad uso poco consapevole della rete. Il termine indica un fenomeno molto frequente tra i giovani che consiste nello scambio di contenuti mediali sessualmente espliciti, spesso i ragazzi lo fanno senza esserne realmente consapevoli di scambiare materiale pedopornografico che potrebbe

arrivare nelle mani sbagliate ed avere conseguenze impattanti emotivamente per i protagonisti delle immagini, dei video, delle foto.

Spesso sono realizzate con il cellulare e vengono diffuse attraverso invio di mms e sms o condivisione tramite bluetooth o attraverso siti e-mail e chat. Sovente tali immagini o video, anche se inviate ad un gruppo ristretto di persone si diffondono in modo incontrollabile e possono creare seri problemi, sia legali che personali ed emotivi alla persona ritratta. L'invio di foto che ritraggono minorenni al di sotto dei 18 anni in pose sessualmente esplicite, configura, infatti il reato di distribuzione di materiale pedopornografico.

I contenuti sessualmente espliciti, quindi possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente vendetta porno fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte **la legge 19 luglio 2019 n°69 art 10**, ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini e video sessualmente espliciti.

Tra le caratteristiche del fenomeno vi sono principalmente

la fiducia tradita: chi produce e invia contenuti sessualmente ripone fiducia nel destinatario, credendo inoltre alla motivazione della richiesta es .prova d'amore, richiesta all'interno di una relazione sentimentale.

la pervasività con cui si diffondono i contenuti in pochi istanti e attraverso una condivisione che diventa virale, il contenuto si diffonde in maniera esponenziale e diventa facilmente modificabile, scaricabile e la sua trasmissione è incontrollabile.

la persistenza del fenomeno, il materiale pubblicato on line, il materiale pubblicato on line può rimanere per un tempo illimitato e può finire con il danneggiare in termini psicologici e sociali i soggetti delle foto e chi li ha diffusi.

4.6 - Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat,

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

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

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

CAPITOLO 4. 6- ADESCAMENTO ONLINE

Il grooming dall'inglese prendersi cura, è una tecnica di manipolazione psicologica che gli adulti abusanti utilizzano per indurre i bambini o gli adolescenti a superare le resistenze emotive e instaurare una relazione intima e o sessualizzata. Gli adulti interessanti sessualmente ai bambini/e adolescenti utilizzano spesso anche gli strumenti messi a disposizione della 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, i siti e le app di teendating, 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 (articolo 609 undecies-l'adescamento di minorenni) quando è stata ratificata la convenzione di Lanzarote legge 172 del 1 ottobre 2012.

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

Potenziati vittime dell' adescamento online possono essere sia bambini che bambine, sia ragazzi che ragazze. Il fenomeno non conosce distinzione di genere.

Gli adolescenti sono particolarmente vulnerabile poichè si trovano in una fase della loro vita in cui è molto importante il processo di costruzione dell'identità sessuale. Anche per questo potrebbero essere aperti e curiosi verso nuove esperienze e attratti da relazioni intime e apparentemente rassicuranti. In questa fase è importante il bisogno di avere attenzioni esclusive da parte di un'altra persona e rinforzi esterni di approvazione per il proprio corpo e la propria immagine. È proprio in ragione della fiducia costruita nella relazione che le vittime di adescamento online riferiscono di sentirsi umiliati, usate, tradite e tendono a sentirsi in colpa ed autosvalutarsi per essere cadute nella trappola.

Il processo di adescamento segue 5 fasi

-fase dell'amicizia iniziale. in questa fase l'adescatore cerca i contatti iniziali con la vittima individuata, provando a socializzare con lei. Tenterà quindi di conoscerla meglio al fine di carpirne i bisogni.

-la fase del risk-assessment in seguito ai primicontatti con il minore, l'adescatore cerca di comprendere il contesto in cui si svolge l'interazione. L'obiettivo dell'adescatore è quello di rendere sempre più privato ed esclusivo il rapporto, cercando di passare ad esempio da una chat pubblica ad una privata, attraverso il telefono per capire il numero.

-fase della costruzione del rapporto di fiducia : le confidenze e le tematiche affrontate divengono via via più private ed intime o comunque molto personali. In questa fase l'adescatore può iniziare a fare regali di vario tipo alla vittima e può anche avvenire uno scambio di foto, subito e non necessariamente a sfondo sessuale.

-fase dell'esclusività: l'adescatore rende la relazione con il minore sempre più segreta isolandolo sempre di più dalla famiglia e dagli amici. Chiederà alla vittima di non raccontare a nessuno ciò che sta avvenendo. L'esperienza reciproca verrà presentata come un geloso segreto da custodire per non rovinare tutto. In questa fase l'adescatore può usare i ricatti morali per non rovinare tutto.

-fase della relazione sessualizzata: in questa fase la richiesta di foto e video a sfondo sessuale può essere più insistente, così come la possibilità di incontri offline. Qualora il minore avesse inviato immagini o video potrebbe essere ricattato dall'adescatore se non accettasse un eventuale incontro con l'adescatore, potrebbe diffondere quel materiale online. Questi tenderà a rappresentare la situazione come normale al fine di vincere eventuali resistenze del minore e coinvolgimenti.

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento del minore. A seguire alcune domande essenziali che possono essere di aiuto.

- il minore ha conoscenze sessuali non adeguate alla sua età

- si viene a conoscenza di un certo video che circola online, o che il minore ha ricevuto, ma c'è imbarazzo nel raccontarlo di più

- il minore si isola e sembra preso solo da una relazione online

- ci sono prese in giro a sfondo sessuale verso un bambino

L'importanza di una adeguata educazione alla sessualità e alla affettività, è il miglior modo per prevenire casi di adescamento online.

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 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](#).

Capitolo 4,7 - Pedopornografia

La pedopornografia online è un reato, art. 600-ter comma 3 del cp, che consiste nel produrre e divulgare, anche per via telematica, immagini o video ritraenti bambini-e ragazzi- ragazze coinvolti in comportamenti sessualmente espliciti 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 ai minori, quali nuove forme di schioavitù". introduce nuove fattispecie di reato e insieme alle successive modifiche e integrazioni contenute nella legge n°38 del 6 febbraio 2006 2 disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo di 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, reato di pornografia minorile virtuale che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/E 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 18 per scopi sessuali.

In un'ottica di attività preventive, il tema della pedopornografia è molto delicato, bisogna cercare informazioni che si possono condividere e che non rechino danni. Il ruolo svolto da generazioni connesse è molto importante, perchè nella sezione "segnala contenuti illegali" (HOT LINE) si può segnalare in anonimato.

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 diggusi attraverso la Rete, I due messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità.

L'abuso sessuale online rappresenta una particolare declinazione dell'abuso sessuale su bambini/e, ragazzi/e, la cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale online si manifesta producono effetti sulle vittime che si aggiungono e moltiplicano a quelli associati all'abuso sessuale. Si pensi, a titolo di esempio, all'impatto che può avere la consapevolezza dell'esistenza (spesso anche in Rete) delle immagini e o video dell'abuso sulla vittima, o a come gestire le stesse immagini e o video durante la fase investigativa e giudiziaria. L'esposizione alle immagini dell'abuso, infatti, sia durante il processo giudiziario, sia durante il percorso di cura, deve essere attentamente valutata, poichè può comportare, per il/la minore coinvolto/a , un rischio di vittimizzazione secondaria.

Negli ultimi anni infine, abbiamo assistito all'emergere di un altro fenomeno che può avere risvolti connessi al fenomeno della pedopornografia: il sexting , di cui abbiamo parlato nelle precedenti lezioni. La mancanza d'intenzione di danneggiare o sfruttare l'altro/a (anche se a volte tale materiale può essere successivamente utilizzato con questo scopo come nel caso del cyberbullismo o del ricatto a fini di estorsioni) non esclude che i comportamenti del sexting possano configurare reati connessi con la pedopornografia poichè, secondo il nostro ordinamento giudiziario, il materiale così prodotto e scambiato si declina come pedopornografico e soprattutto perchè il rischio di perdere il controllo di tali immagini, uscendo dallo scambio consensuale è molto alto e spesso ragazzi e ragazze non consapevolezza delle conseguenze delle loro azioni come la possibilità di diffondere in rete immagini intime fuori dai canali riservati allo scambio.

x

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

.

Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.

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

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

Scegliere almeno 1 di queste azioni:

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

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

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

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

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

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

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

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

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

- **Cyberbullismo:** è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenni e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per

segnalare la presenza di materiale pedopornografico online.

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

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

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

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto

Generazioni Connesse, al numero gratuito [1.96.96](tel:19696).

5.3. - Gli attori sul territorio

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

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

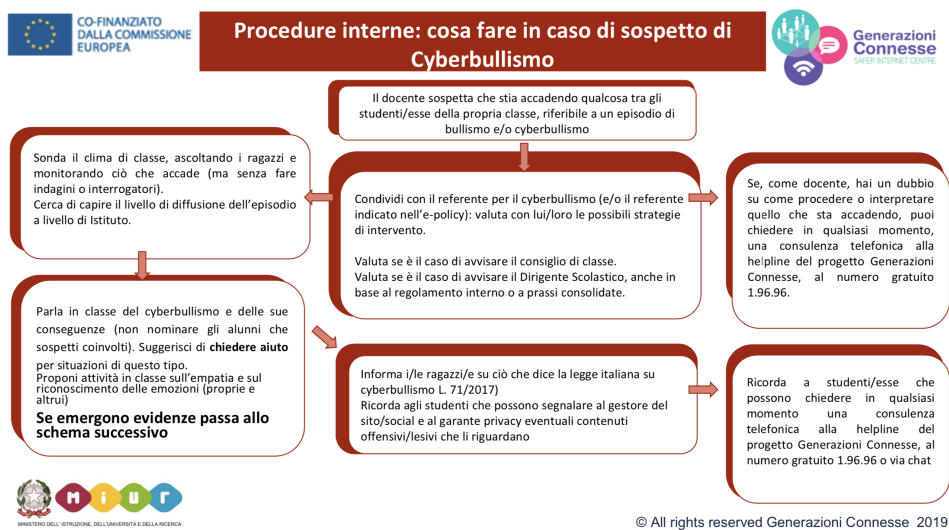
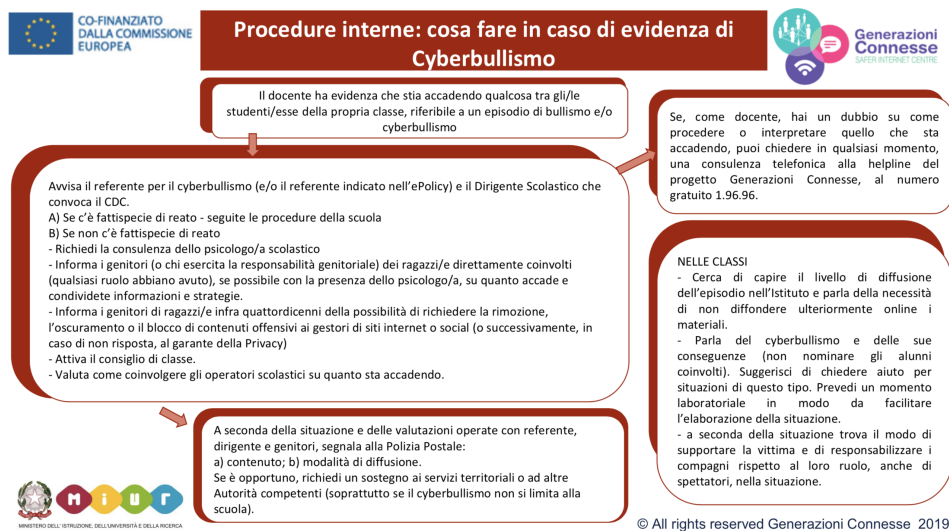
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all’utilizzo di Internet può presentare.

- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell’infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all’uso di Internet.
- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell’utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l’Infanzia e l’Adolescenza e Difensore Civico:** segnalano all’Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

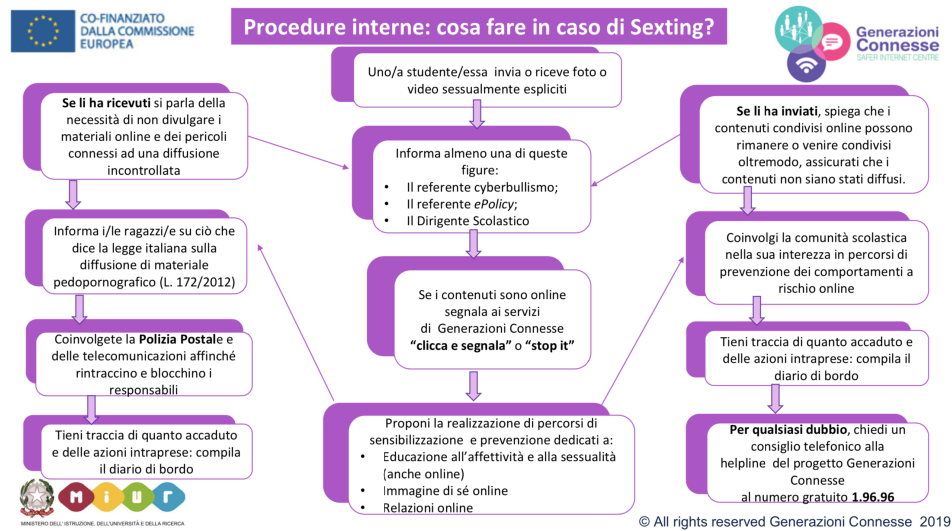
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

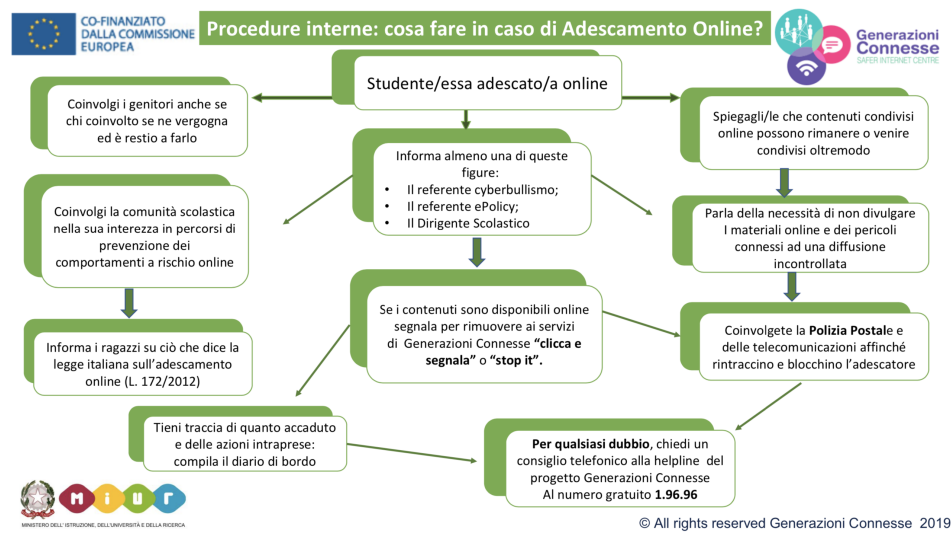
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



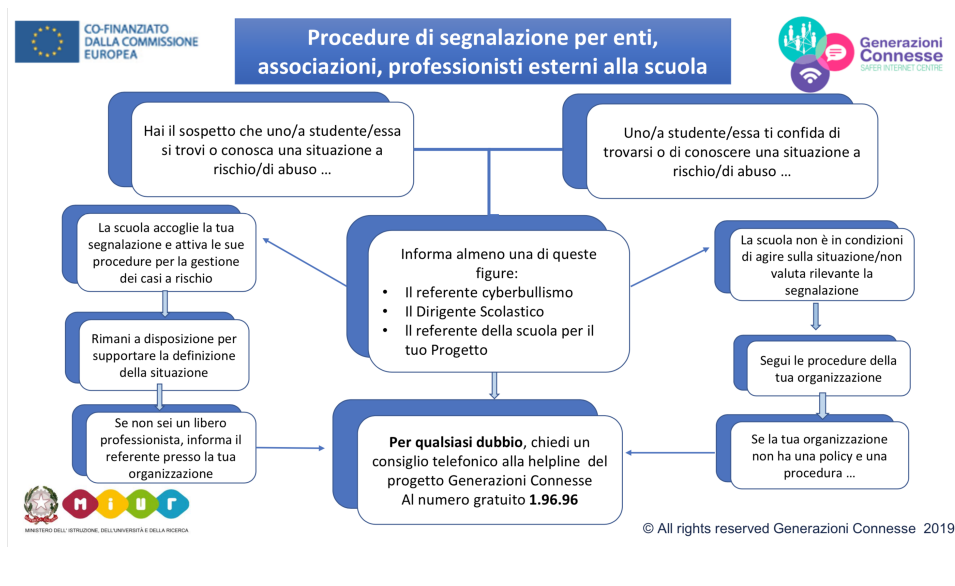
Procedure interne: cosa fare in caso di sexting?



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 reati procedibili d'ufficio](#)

Il nostro piano d'azioni

