



Documento di ePolicy

CLIC81000V

"S. QUASIMODO" - GELA -

VIALE INDIPENDENZA 130 - 93012 - GELA - CALTANISSETTA (CL)

Viviana Morello

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.

1.2 - Ruoli e responsabilità

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

Il Dirigente scolastico promuove ed attiva buone prassi secondo le indicazioni del M.I.U.R., mediante l'organizzazione di percorsi di formazione per la sicurezza e problematiche connesse all'utilizzo della rete sia online che offline, con la collaborazione del docente Referente d'Istituto per le tematiche del Bullismo e del Cyberbullismo, fermo restando la responsabilità di gestire ed intervenire nei casi di gravi episodi ed uso improprio delle tecnologie digitali degli studenti e delle studentesse.

Il Referente d'Istituto per la prevenzione ed il contrasto del Bullismo e del Cyberbullismo, individuato ai sensi dell'art. 4, comma 3, Legge 29 maggio 2017, n.71, ha il compito di "coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio". Il suo ruolo è fondamentale non solo in ambito scolastico ma anche in quello extrascolastico - ove possibile -, per il coinvolgimento di percorsi formativi finalizzati per studenti e studentesse, per genitori e per l'intera comunità scolastica.

I docenti hanno un ruolo centrale nel "diffondere la cultura dell'uso responsabile delle TIC e della Rete", accostando alla didattica l'utilizzo delle tecnologie digitali, ove possibile. 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 al Dirigente scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse". In particolare, si impegnano a: informarsi e ad aggiornarsi su tema della sicurezza in rete uniformandosi alle politiche di sicurezza adottate dalla scuola di cui rispettano il regolamento; supportare gli alunni nel corretto utilizzo delle tecnologie digitali per finalità didattico-educative (controllo nel rispetto delle leggi, del regolamento interno, del plagio, del diritto d'autore, ecc.); a

guidare gli studenti nella scelta della fonte di informazioni; a garantire che le comunicazioni con i mezzi informatici avvengano nel rispetto dei ruoli e dei rispettivi codici comportamentali, mediante canali ufficiali e verificabili (registro elettronico, piattaforma G-suite per la DDI, ecc.); a rispettare l'obbligo di riservatezza dei dati personali trattati e non, in conformità alla normativa vigente; a interagire con i genitori, coordinando con gli stessi l'intervento educativo, nei casi di disagio, manifestato dall'alunno, collegato all'utilizzo delle tecnologie digitali; a segnalare al Dirigente Scolastico eventuali criticità nei sistemi informativi, soprattutto in materia di prevenzione e gestione dei rischi nell'uso delle TIC; a segnalare al Dirigente Scolastico eventuali abusi subiti dagli alunni e connessi all'uso delle tecnologie digitali.

Il Personale Amministrativo, Tecnico ed Ausiliario (ATA), svolge funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza, connesse alle attività dell'Istituzione scolastica, in collaborazione con il Dirigente scolastico e con il personale docente tutto. È coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo insieme alle figure interne preposte, e nel raccogliere, verificare e valutare le informazioni inerenti a possibili casi di bullismo e di cyberbullismo.

Gli studenti e le studentesse sono tenuti/e al rispetto delle norme che disciplinano l'utilizzo consapevole delle tecnologie digitali con la finalità di salvaguardare la propria identità e quella altrui, secondo quanto indicato nei Regolamenti di Istituto. Ad essi è richiesto di: utilizzare responsabilmente le tecnologie digitali uniformandosi alle indicazioni dei docenti nonché rispettando le norme codificate nei regolamenti di istituto; a rispettare le buone pratiche di sicurezza in rete; a saper distinguere, con l'aiuto dei docenti, le fonti di informazione attendibili in rete per utilizzarle in modo appropriato senza violazione dei diritti d'autore altrui; a comunicare in rete in modo appropriato rispettando le posizioni altrui; a segnalare ai genitori e/o ai docenti situazioni di difficoltà o di bisogno di aiuto nell'utilizzo delle tecnologie digitali.

I genitori sono corresponsabili nelle scelte educative dell'Istituzione scolastica, atte alle attività di prevenzione ed uso consapevole delle TIC, della Rete e dei devices personali dei rispettivi figli. Ad essi è richiesto di sostenere i docenti nell'azione educativa diretta al corretto utilizzo delle tecnologie digitali; ad educare (vigilando sui propri figli) al corretto utilizzo delle tecnologie digitali in ambiente domestico fissando regole comportamentali e di utilizzo; a collaborare con i docenti nell'adozione di linee di intervento coerenti per contrastare l'uso non responsabile, scorretto o pericoloso delle tecnologie digitali.

Gli Enti educativi esterni e le Associazioni che entrano in relazione con l'Istituzione scolastica osservano le politiche interne sull'uso consapevole della Rete e delle TIC, fermo restando di attivare procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse, durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

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).

da compilare con le indicazioni contenute nella lezione

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 E-Policy è stato redatto dal gruppo di lavoro composto dalla Prof.ssa Rosaria Albini, Docente e dall'a.s. 2020/2021 Referente per la prevenzione ed il contrasto del bullismo e cyberbullismo, dalla Prof.ssa Maria Grazia Piparo e dal Prof. Salvatore di Blasi. La Prof.ssa Viviana Morello è il Dirigente Scolastico. I docenti componenti il gruppo di lavoro hanno seguito una formazione online apposita ai fini della redazione di tale documento.

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.

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.

da compilare con le indicazioni contenute nella lezione

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.

da compilare con le indicazioni contenute nella lezione

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

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.

Nel nostro Istituto la presenza e l'utilizzo di strumenti tecnologici sono ormai una realtà consolidata da anni nella consapevolezza che la scuola digitale vada pensata non solo in funzione dell'innovazione fine a se stessa, ma anche e soprattutto delle concrete finalità didattiche.

In esecuzione del decreto ministeriale dell'11 marzo 2016, prot. n. 157, il M.I.U.R. ha promosso la realizzazione di Curricoli Digitali da parte delle istituzioni scolastiche ed educative statali, favorendo esperienze di progettazione partecipata, al fine di creare, sperimentare e mettere a disposizione di tutte le scuole nuovi curricula didattici innovativi, strutturati, aperti e in grado di coinvolgere la comunità scolastica allargata.

Il curriculum digitale è concepito come un percorso didattico verticale che, nei due ordini di scuola, permetta agli alunni di sviluppare competenze digitali interdisciplinari di facile replicabilità, utilizzo e applicazione su più fronti, muovendo da cinque aree

fondamentali:

Informazione: identificare, localizzare, recuperare, conservare, organizzare e analizzare le informazioni digitali, giudicarne attendibilità, importanza e scopo;

Comunicazione: comunicare in ambienti digitali, condividere risorse attraverso strumenti online, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire e partecipare alle comunità e alle reti;

Creazione di contenuti: creare e modificare nuovi contenuti, integrare e rielaborare le conoscenze e i contenuti, produrre espressioni creative e contenuti media, conoscere e applicare i diritti di proprietà;

Sicurezza: protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile;

Problem solving: identificare i bisogni e le risorse digitali, prendere decisioni informate sui più appropriati strumenti digitali secondo lo scopo e la necessità, utilizzare creativamente le tecnologie, risolvere problemi tecnici, aggiornare la propria competenza.

Avendo la competenza digitale carattere trasversale a tutte le discipline, l'attuazione del curricolo digitale vede coinvolti tutti gli insegnamenti e i campi di esperienza e può essere applicata ad una molteplicità di attività didattiche e di interventi metodologici.

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.

La professione docente è complessa e pertanto richiede competenze diverse ed integrate, fra queste anche quelle di tipo digitale. Le TIC, infatti, 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 e le studentesse 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, tenendo presente l'immagine che fornisce in merito il DigComp: "imparare a nuotare nell'oceano digitale". La metafora fornita dal documento indica che è necessario sapersi destreggiare, partendo dai compiti semplici (es.: individuare i fabbisogni informativi; trovare dati, informazioni e contenuti attraverso una semplice ricerca in ambienti digitale etc.) per arrivare ai compiti complessi che presentano molti fattori di interazione (ad es.: creare nuove app o piattaforme per navigare, ricercare e filtrare portali e offerte).

È su tali premesse che l'Istituto, attraverso il collegio dei docenti, riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (con l'aiuto dell'animatore digitale) dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online), purché restino coerenti con il piano di formazione.

Fondamentale, infatti, che vi sia attenzione all'uso delle TIC nella didattica: un loro utilizzo strutturato e integrato non solo può rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi, ma permette al docente di guidare gli alunni rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento al di fuori della scuola. Inoltre, permettono di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona.

La competenza digitale, oggi, è imprescindibile per i docenti così come per gli alunni e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento, cogliendo tale sfida anche grazie alla possibilità di formazione permanente offerta loro in primis dall'Istituto scolastico, in modo da rispondere ai diversi bisogni formativi della classe.

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.

A questo proposito è necessario e auspicabile che i docenti tutti dell'Istituto scolastico seguano un percorso formativo specifico ed adeguato che abbia ad oggetto non solo l'uso responsabile e sicuro della Rete ma anche i rischi legati a quest'ultime.

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

Per tali ragioni, la nostra scuola prevede specifici momenti di formazione permanente per gli insegnanti che mettano al centro i temi in oggetto, considerando anche percorsi di autoaggiornamento personali o collettivi, iniziative seminariali con professionisti-esperti interni (l'Animatore digitale) ed esterni alla scuola, giornate-settimane di approfondimento in accordo con la rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), le amministrazioni comunali, i servizi socio-educativi e le associazioni/enti presenti. Tali azioni programmatiche vengono inserite nel Piano triennale dell'offerta formativa.

Vengono organizzati anche momenti formativi di approfondimento (progetti specifici, laboratori, eventi, giornate, etc, ...) con le famiglie in modo da sensibilizzare l'intera comunità educante sia su

un corretto uso delle tecnologie digitali sia sulle potenzialità della Rete.

I momenti di formazione e aggiornamento sono pensati e creati a partire dall'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica; dall'analisi del fabbisogno conoscitivo circa particolari argomenti che si sentono come più cogenti per i docenti e l'Istituto; dall'analisi delle richieste che provengono dagli studenti e dalle studentesse in modo, poi, da riutilizzarli nel loro lavoro di educatori (attraverso le modalità che il docente indica e ritiene più confacente alla classe) quanto appreso durante la formazione ricevuta attraverso un cronoprogramma che consideri il triennio scolastico, in un'ottica di vera e propria programmazione, con azioni specifiche. Le azioni sono le seguenti:

1. Analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;

2. Promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse".
3. Monitorare le azioni svolte per mezzo di specifici momenti di valutazione;
4. Organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.

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

Sempre sul sito istituzionale della scuola, saranno inclusi link e materiali informativi del progetto "**Generazioni connesse**", a partire dall'inserimento del link del progetto: www.generazioniconnesse.it/ dove trovare ulteriori approfondimenti, spunti aggiornamenti e strumenti didattici utili da usare con gli alunni.

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.

Oggi più che mai è importante rinforzare l'alleanza educativa fra scuola e famiglie.

Per questo motivo è importante il coinvolgimento delle famiglie nell'educazione digitale degli alunni, con percorsi da mettere in pratica insieme per sensibilizzare i genitori sulle tematiche relative alle TIC.

In tal senso verrà integrato, oltre che il regolamento scolastico, anche il "Patto di corresponsabilità", con specifici riferimenti alle tecnologie digitali e all'ePolicy.

Il "Patto di Corresponsabilità" è un documento centrale per ogni istituzione scolastica e per la comunità educante tutta. Per questo, recentemente è stato avviato dal Miur un percorso di revisione finalizzato a definire in modo più dettagliato modalità, tempi e ambiti della partecipazione da parte di genitori e studenti alla vita scolastica. E ciò, anche al fine di creare una maggiore collaborazione e condivisione degli interventi di formazione e di contrasto al bullismo e al cyberbullismo all'interno della comunità educante.

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

Il "Patto di corresponsabilità" verrà aggiornato con specifici riferimenti all'uso delle tecnologie digitali e all'ePolicy diventando così fondamentale, per informare e rendere partecipi le famiglie sul percorso intrapreso con il documento e il piano d'azione.

E' 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.

La nostra scuola si propone di:

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

Sarà dedicata particolare attenzione a consigli, indicazioni e informazioni su iniziative e azioni della scuola, in riferimento ai rischi connessi ad un uso distorto della Rete da parte degli alunni.

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

meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

Scegliere almeno 1 di queste azioni

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

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie

digitali.

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

La protezione dei dati personali è, infatti, 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 particolare, la scuola non ha solo il compito di tutelare la privacy degli alunni e delle loro famiglie, ma anche quello di informarli e soprattutto renderli consapevoli di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

La diffusione sempre maggiore di smartphone tra i giovanissimi, l'uso di tablet a scopo didattico, la condivisione online di contenuti didattici, l'uso del registro elettronico, l'eventualità di gruppi whatsapp tra genitori e docenti, obbliga la scuola ad avere un'attenzione particolare non solo alla privacy in generale, ma anche alla gestione della privacy legata all'uso dei nuovi dispositivi. La velocità, l'immediatezza con cui si risponde ai messaggi o si condividono foto o video, può far perdere il controllo di dati personali e mettere a rischio la reputazione e la sicurezza dei soggetti coinvolti.

I dati personali

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.

Fra questi, particolarmente importanti sono:

- i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati cosiddetti sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679

(articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;

- i dati relativi a condanne penali e reati: si tratta dei dati cosiddetti giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitiva, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle tecnologie digitali, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geo-localizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti di una persona.

La "protezione dei dati personali"

Gli attori che entrano in gioco nella protezione dei dati personali sono:

L'interessato: è la persona fisica alla quale si riferiscono i dati personali (art. 4, paragrafo 1, punto 1), del Regolamento UE 2016/679);

Il titolare: è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico, privato o l'associazione che adotta le decisioni sugli scopi e sulle modalità del trattamento (art. 4, paragrafo 1, punto 7), del Regolamento UE 2016/679);

Il responsabile: è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati (art. 4, paragrafo 1, punto 8), del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. sub-responsabile (art. 28, paragrafo 2).

Il trattamento dei dati

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

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

Obblighi delle scuole in tema di protezione dei dati personali

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti non sono tenute a chiedere il consenso degli/le studenti/esse.

Alcune categorie di dati personali degli alunni e delle famiglie, come quelli sensibili e giudiziari, devono essere trattate con estrema cautela, nel rispetto di specifiche norme di legge, verificando in primis non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire.

Esempi di violazione sono il trattamento dei dati senza aver fornito all'interessato un'adeguata informativa o senza aver ottenuto uno specifico e libero consenso, qualora previsto.

In tali casi la persona interessata (genitore, professore, etc.) può presentare al [Garante per la Protezione dei dati personali](#) un'apposita "segnalazione" gratuita o un "reclamo" (più circostanziato rispetto alla semplice segnalazione e con pagamento di diritti di segreteria).

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

Per cui l'Istituzione scolastica dovrà:

Redigere e mantenere un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti.

Effettuare una valutazione dei rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili. L'istituzione scolastica può trattare anche dati sensibili, come ad esempio dati relativi alle origini razziali per favorire l'integrazione degli alunni, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli alunni, come i dati vaccinali con le Asl.

Effettuare un'analisi di processo sulla raccolta/gestione del consenso: occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio, all'interno di modulistica o sul proprio sito web istituzionale. La formula utilizzata per chiedere il consenso deve essere comprensibile, semplice e chiara (art. 7.2). La scuola non deve, di regola, chiedere il consenso per il

trattamento dei dati personali, ma deve adeguare tutta la modulistica al Regolamento

UE 2016/679 e predisporre una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.

Predisporre l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti:

Analisi del sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati:

A tale proposito

1. è stata effettuata la migrazione del sito dal suffisso gov.it (non più valido per le istituzioni scolastiche secondo la determina n. 36 del 12 febbraio 2018) al suffisso edu.it;
2. la progettazione del nuovo sito è stata fatta secondo i concetti di [privacy by default e by design](#);
3. viene utilizzato il protocollo HTTPS (l'Hypertext Transfer Protocol Secure è un protocollo per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati online);
4. viene utilizzato di un sistema di cifratura quando il trattamento di dati lo richiede (ovvero oscurare il dato per renderlo incomprensibile a coloro che non hanno i codici per accedervi, mediante la "crittografia" e, quindi, l'uso di un algoritmo di cifratura);
5. è attivo il sistema di backup (sistema che permette di salvare regolarmente i dati; ripristinare eventuali file modificati o rimossi per errore dalla rete; garantire la presenza di una copia di sicurezza di tutti i file importanti);
6. è attivo il piano di disaster recovery (insieme di misure che permettono agli apparati di Information technology di superare situazioni di emergenza, ovvero di impedire che imprevisti accidentali o incidenti possano compromettere il funzionamento delle strutture).

La messa in sicurezza della intranet scolastica è stata predisposta:

1. sulle reti Wi-fi installate;
2. tramite utilizzo di [white list](#) per la navigazione (sistemi di filtraggio dei contenuti);
3. tramite utilizzo di un proxy che permette di fornire un maggiore anonimato durante la navigazione in Rete, funziona da antivirus e memorizza una copia locale degli elementi web;
5. tramite uso di un firewall hardware ;
6. istituendo corsi di formazione destinati ai responsabili, agli incaricati ed eventualmente ai sub- incaricati del trattamento.

La Liberatoria

La scuola non è tenuta a richiedere alle famiglie l'autorizzazione alle riprese

fotografiche e video solo se esse sono realizzate a fini personali e non a fini di pubblicazione o divulgazione. Nel caso che le suddette immagini vengano divulgate sul sito della scuola o sui social network è necessaria l'autorizzazione degli interessati.

In generale il Garante per la protezione dei dati personali stabilisce che "le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano.

Le famiglie hanno il diritto di conoscere quali informazioni sono trattate dall'Istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

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.

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. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il 'diritto a Internet' diventi una realtà, a partire dalla scuola".

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

Per garantire tale diritto, a scuola due sono gli aspetti da tenere in considerazione:

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

In quest'ottica, accanto al monitoraggio di opportunità in tal tramite bandi PON o europei, si cercherà di coinvolgere anche l'amministrazione locale.

L'adeguamento della rete intranet della scuola è necessario anche in previsione di un potenziamento degli strumenti didattici e laboratoriali necessari a migliorare la formazione e i processi di innovazione delle istituzioni scolastiche e all'adozione di strumenti organizzativi e tecnologici che permettano un'amministrazione trasparente, la condivisione di dati e la dematerializzazione degli atti, oltre al fondamentale scambio di informazioni tra dirigenti, docenti, famiglie, permesso dal registro elettronico.

Un ambiente sicuro anche online

In inglese esistono due termini per parlare di sicurezza: il primo termine è safety e riguarda la prevenzione dei rischi, a partire dalla consapevolezza, conoscenza e preparazione per un uso consapevole delle tecnologie digitali (ed è questo l'approccio del progetto "Generazioni Connesse"). L'altro termine è security che, in relazione ad

Internet e ai media, si riferisce a tutte quelle risorse tecnologiche che rendono sicuro l'ambiente digitale, dall'antivirus al firewall, da un protocollo di trasmissione dei dati sicuro (https) all'aggiornamento di software e sistemi operativi.

La nostra scuola considera l'ambiente online alla stregua dell'ambiente fisico e ne valuta tutti gli aspetti legati alla sicurezza nel momento in cui permette a alunni e docenti l'accesso alla rete tramite i dispositivi della scuola, tramite la rete scolastica o tramite i dispositivi personali nel caso del BYOD (Bring your own device)

In riferimento alla security non presta attenzione solo all'infrastruttura hardware e alla rete (wireless e non), ma anche alla sicurezza di tutti gli aspetti che riguardano la gestione degli account degli utenti (in modo differenziato tra alunni, insegnanti e personale amministrativo), il filtraggio dei contenuti differenziato in base all'età e gli aspetti legali in relazione prevalentemente alla privacy.

La formazione sull'uso della tecnologia

Per superare la diffidenza nei confronti delle tecnologie a scuola e il divario nell'accesso, siamo andati oltre la possibile prima barriera che ne inibisce un uso efficace da parte di tanti docenti: i problemi tecnici e la scarsa familiarità con la strumentazione.

Per affrontare proattivamente la questione la scuola provvede a pianificare interventi periodici di manutenzione e tiene anche un registro delle problematiche incontrate per poter stilare una classifica dei problemi più frequenti. Questo aspetto è fondamentale per la formazione degli insegnanti in quanto permettere loro di affrontare e risolvere in autonomia tutte quelle situazioni e casistiche di mal funzionamento dei dispositivi che si possono presentare nella quotidianità. La formazione non riguarderà solo l'uso delle tecnologie digitali nella didattica, ma anche il funzionamento e l'uso stesso della tecnologia in sé.

La scuola si è dotata della seguente checklist per garantire la cybersecurity

- Mantenere separate le reti didattica e segreteria: importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall.
- Aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline).
- Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
- Testare regolarmente le possibili vulnerabilità.
- Preparare piani di azione in risposta ai problemi più seri: è importante non

dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione.

- Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo: se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate.
- Impostare il browser per l'eliminazione dei cookies alla chiusura: in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione.
- Definire una policy sulle password: le password devono essere forti:
 - Richiedere password complesse con almeno 8 caratteri con numeri, maiuscole e minuscole e caratteri speciali.
 - Sensibilizzare rispetto al non uso di password facilmente identificabili;
 - Non memorizzare le password nei dispositivi scolastici.
 - Non condividere le password con nessuno.
- Minimizzare i privilegi amministrativi: solo poche persone autorizzate dovrebbero avere privilegi amministrativi. La maggior parte dei docenti possono accedere con account con permessi limitati.
- Sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile): deve riguardare chiunque abbia accesso alla Rete, alunni, docenti, amministrazione e segreteria, includere i dispositivi della scuola e quelli personali, anche in caso di BYOD.

Infine, in sintesi, un elenco di: buone pratiche nell'uso della rete, linee guida di buona condotta dell'utente, regole che disciplinano l'accesso a INTERNET. Buone pratiche nell'uso della rete:

- Controllo della validità e dell'origine delle informazioni a cui si accede o che si ricevono;
- Utilizzo di fonti alternative di informazione per proposte comparate;
- Ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale e di altri possibili link al sito;
- Rispetto dei diritti di autore e dei diritti di proprietà intellettuale.

Linee guida di buona condotta dell'utente

- Rispettare la legislazione vigente;
- Tutelare la propria privacy, quella degli altri utenti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui hai accesso;
- Rispettare la cosiddetta netiquette (regole condivise che disciplinano il rapportarsi fra utenti della rete, siti, forum, mail e di qualsiasi altro tipo di comunicazione).

Le regole

- Rispettare le persone diverse per nazionalità, cultura, religione, sesso;
 - Non rivelare dettagli o informazioni personali o di altre persone (indirizzi, numeri di telefono);
 - Richiedere sempre il permesso prima di iscriversi a qualche mailing-list o sito web;
 - Non dare indirizzo e numero di telefono a persone incontrate sul web;
 - Non prendere appuntamenti con le persone conosciute tramite web;
 - Non inviare fotografie proprie o di altre persone;
 - Riferire sempre a insegnanti e genitori se si incontrano in Internet immagini o scritti che infastidiscono;
 - Se qualcuno non rispetta queste regole è necessario parlarne con genitori ed insegnanti;
 - Chiedere il permesso prima di scaricare dal web materiale di vario tipo.
-

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.

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. Sono diversi, infatti, gli strumenti di comunicazione online che possono essere utilizzati a scuola, integrando quelli più tradizionali e che possono rendere lo scambio comunicativo maggiormente interattivo e orizzontale. La sfida, allora, è quella di conoscere al meglio tali strumenti, sfruttarne le potenzialità e come sempre prevenire eventuali rischi correlati ad un uso poco consapevole degli stessi.

Grazie all'uso delle tecnologie digitali, da una comunicazione uno a molti, si può passare ad una comunicazione che per definizione può essere molti a molti, multimediale, bidirezionale e interattiva. Ciò naturalmente può rappresentare un'opportunità significativa anche in termini di un maggiore coinvolgimento degli alunni o dei genitori, o alla possibilità di usare diversi linguaggi (scrittura, immagini, video etc.) ma in taluni casi può anche rivelarsi un problema non sempre facile da gestire, ad esempio, l'uso talvolta smodato e senza regole che docenti, ragazzi o genitori fanno dei gruppi whatsapp.

Le caratteristiche della comunicazione messa in atto attraverso le tecnologie digitali e l'uso della Rete (quella che comunemente viene definita la Computer mediated communication) si differenzia sostanzialmente dalla cosiddetta comunicazione face to face. Ciò ha implicazioni molto importanti su come gli strumenti di comunicazione online devono essere utilizzati a scuola, sulle regole per il loro uso, e sulle tipologie di comunicazione che si vogliono implementare attraverso di essi. Non tutte le forme di comunicazione, infatti, sono adatte a viaggiare online perché, talvolta, il fraintendimento è dietro l'angolo o la tentazione dell'essere always on (sempre connessi) può essere più forte e degenerare in inutile stress.

Le caratteristiche della comunicazione mediata dalle tecnologie

Quando ci relazioniamo attraverso l'uso di strumenti di comunicazione online, mettiamo in atto una modalità comunicativa che ha caratteristiche e logiche proprie. Ecco, allora, alcuni aspetti importanti da tenere in considerazione e di cui è importante essere consapevoli quando si fa uso delle TIC nelle comunicazioni a scuola.

Nella comunicazione mediata dalle tecnologie non condividiamo lo stesso spazio e lo stesso contesto comunicativo con i nostri interlocutori. Per questo può accadere che si forniscano cornici interpretative molto diverse ai messaggi e ai contenuti scambiati. Essa, inoltre, generalmente non ci permette di accedere ai cosiddetti segnali della comunicazione non verbale (tono della voce, espressione del volto, gesti del corpo, pause...etc.) e non siamo in grado di vedere ed ascoltare direttamente gli effetti della nostra comunicazione sull'interlocutore. Ciò comporta che difficilmente potremo adeguare il nostro comportamento a partire da tali segnali. Il cosiddetto feed-back non tangibile e l'impossibilità di accedere ai segnali non verbali del nostro interlocutore, così come la distanza e la separazione mediante lo schermo, ci rendono meno empatici e quindi meno attenti a emozioni e potenziali reazioni dell'altra persona. Inoltre, la comunicazione che viaggia online, generalmente, si avvale di messaggi scritti che possono essere memorizzati, diffusi e permangono nel tempo. È sempre bene tenerlo a mente.

D'altro canto, grazie agli strumenti di comunicazione online, come già in parte sottolineato, possiamo usufruire dell'interattività del mezzo, superare le barriere spazio-temporali, usare un linguaggio multimediale, ipertestuale e accattivante, promuovere la partecipazione e il coinvolgimento dei diversi attori in gioco nel processo educativo (dai ragazzi ai genitori). Diversi sono gli strumenti di comunicazione online che possono essere utilizzati dalla scuola, sia per raggiungere target esterni, al fine di valorizzare e promuovere le attività portate avanti dall'Istituto (rivolgendosi ad esempio a istituzioni, famiglie, associazioni etc.) sia per far circolare all'interno della scuola informazioni di servizio o contenuti importanti fra i diversi attori scolastici (docenti, genitori, collaboratori scolastici etc.).

Fra gli strumenti di comunicazione esterna, troviamo in primis il sito web della scuola, eventuali profili sui social network (si pensi a Facebook, Instagram, LinkedIn, Twitter, Youtube), la newsletter, il blog, una web-radio o una web tv scolastica. Tali strumenti,

naturalmente, possono essere utilizzati anche per fornire informazioni di servizio rivolte a studenti o genitori. In quest'ottica la comunicazione esterna online della scuola sarà coordinata e progettata a partire da un piano di comunicazione in grado di trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che il nostro Istituto porta avanti e a partire dalla condivisione di regole ben precise su cosa comunicare e come comunicarlo. La comunicazione esterna dell'Istituto sarà progettata ed implementata anche con il supporto dei docenti che potrebbero produrre contenuti multimediali da diffondere attraverso i vari canali in uso (video, foto, post sui social, articoli per il sito o per il blog etc.).

Fra gli strumenti di comunicazione interna, invece, troviamo il registro elettronico con tutte le sue funzionalità, la classica e-mail, gli strumenti di messaggistica istantanea che però hanno sempre più funzionalità tipiche anche dei social network, whatsapp o telegram, i gruppi Facebook, o ulteriori applicativi e piattaforme di lavoro condiviso e collaborativo come [wiki](#), [google doc](#), [classroom](#) che possono essere ampiamente utilizzati anche per facilitare e rendere più partecipata la didattica e la comunicazione a scuola.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne, come avviene generalmente fra i docenti mediante ad esempio l'uso di gruppi whatsapp o telegram, è importante ricordare quello che si può definire "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare. È importante sottolineare però che per le chat informali fra colleghi, o fra docenti e genitori, non esiste una vera e propria regolamentazione, e per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, che si elaborino regole condivise sull'uso delle stesse. Fra queste, ad esempio:

- Mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi fraintendimenti);
- Evitare di affrontare in chat argomenti troppo complessi e controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
- Evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- Non condividere file multimediali troppo pesanti;
- Evitare il più possibile di condividere foto di alunni in chat;
- Indirizzare solo domande precise e chiare, a cui si possano dare risposte

altrettanto brevi e precise;

- Evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo.

Quando si usano invece chat formali, create ad esempio dal Dirigente scolastico per veicolare messaggi, informazioni e aggiornamenti relativi all'attività scolastica, la regolamentazione è prevista dalla contrattazione di Istituto.

Altro strumento ormai centrale a disposizione delle scuole per la gestione di assenze, presenze, valutazioni, prenotazioni di incontri e comunicazioni con le famiglie è il registro elettronico.

Il registro elettronico permette di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su:

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

A tal proposito si sta cercando di utilizzare tale strumento sfruttandone appieno le potenzialità, al fine di rendere quanto più immediate, trasparenti ed efficaci le comunicazioni all'interno della scuola e fra scuola e famiglie.

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.

Da implementare con le indicazioni contenute nella lezione.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).**Scegliere almeno 1 di queste azioni:**

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli
- studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Le Tecnologie dell'Informazione e della Comunicazione (TIC) sono parte integrante della vita quotidiana dei più giovani, in quanto strumenti privilegiati di comunicazione e di relazione, ma anche di informazione, studio, creatività e partecipazione. Esse pongono però delle questioni associate alla "sicurezza" e al comportamento sociale che non bisogna trascurare. Gli adulti, dunque la famiglia e la scuola, hanno

la responsabilità di promuovere presso i più giovani un uso consapevole delle tecnologie digitali nelle realtà complessa nella quale viviamo e nella quale trovano spazio contenuti e comportamenti potenzialmente dannosi.

L' I.C.S. "S. Quasimodo" intende perseguire azioni di prevenzione e di sensibilizzazione, attraverso un'efficace integrazione con la rete dei servizi territoriali locali (Polizia Postale, ASP, associazioni di volontariato), al fine di formare e consolidare le competenze educative di base necessarie a poter gestire le situazioni di vita che i ragazzi sperimentano online.

Le azioni di sensibilizzazione riguarderanno:

- accrescere la consapevolezza nel gruppo target di riferimento circa un determinato tema/bisogno/problema che potrebbe presentarsi in quel gruppo;
- incoraggiare il gruppo a modificare i propri comportamenti rendendoli più funzionali;
- diffondere all'esterno del gruppo di riferimento e quindi tra l'opinione pubblica una certa consapevolezza rispetto all'argomento di interesse;
- facilitare il coinvolgimento di soggetti esterni in modo da mettere insieme diverse idee per lavorare ad un obiettivo comune;
- promuovere la conoscenza dell'ePolicy nella comunità scolastica.

Le azioni di prevenzione, volte a contrastare bullismo e cyberbullismo, riguarderanno:

- integrare nel curriculum temi legati al corretto utilizzo delle TIC e di Internet
- supportare e implementare la competenza digitale in tutti i ragazzi all'interno delle materie curriculari.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di [cyberbullismo](#) e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
 - Ha il compito di coordinare le iniziative di prevenzione e contrasto del [cyberbullismo](#). A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
 - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il cyberbullismo è una forma di prepotenza virtuale messa in atto attraverso l'uso di Internet e delle tecnologie digitali.

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

1. cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei.
2. cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

Alcuni segnali generali che la potenziale vittima di cyberbullismo può manifestare sono:

- Appare nervosa quando riceve un messaggio o una notifica;
- Sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);
- Cambia comportamento ed atteggiamento in modo repentino;
- Mostra ritrosia nel dare informazioni su ciò che fa online;
- Soprattutto dopo essere stata online, mostra rabbia o si sente depressa;

- Inizia ad utilizzare sempre meno Pc e telefono (arrivando ad evitarli);
- Perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- Il suo rendimento scolastico peggiora.

Il cyberbullismo non è una problematica che riguarda unicamente vittima e cyberbullo. È un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari.

Responsabilità della famiglia e della scuola

Responsabilità della famiglia

Se il minore non ha compiuto i 14 anni, non risponde penalmente per l'evento, ma i genitori saranno tenuti al risarcimento del danno, per presunta "culpa in educando", così come previsto dal codice civile, per i fatti commessi dal figlio. Non c'è responsabilità penale dei genitori, perché la responsabilità penale è personale.

Responsabilità della scuola

Se si verificano comportamenti penalmente rilevanti a scuola o durante una gita scolastica, interviene l'art. 2048 del Codice Civile (responsabilità dei precettori) e l'art. 61 della L. 312/1980 n. 312 (responsabilità patrimoniale del personale direttivo, docente educativo e non docente). In base a queste norme, quindi, gli insegnanti sono responsabili dei danni causati a terzi "dal fatto illecito dei loro allievi... nel tempo in cui sono sotto la loro vigilanza".

Se si tratta di una scuola pubblica, la responsabilità si estende alla pubblica amministrazione, che si surroga al suo personale nelle responsabilità civili derivanti da azioni giudiziarie promosse da terzi. Se si tratta di una scuola privata, sarà la proprietà dell'Istituto a risponderne. Gli insegnanti potranno essere chiamati a rispondere personalmente solo in caso di azione di rivalsa per dolo o colpa grave, da parte dell'amministrazione. L'insegnante ha un dovere di vigilanza e di conseguenza viene addebitata, in caso di comportamento illecito del minore affidato, una colpa presunta, cioè una "culpa in vigilando", come inadempimento dell'obbligo di sorveglianza sugli allievi. Di questa colpa/responsabilità si può essere liberati dimostrando di non aver potuto impedire il fatto. Si tiene conto in questi casi dell'età e del grado di maturità dei ragazzi, della concreta situazione ambientale, etc.

Inoltre, l'insegnante deve dimostrare di aver adottato in via preventiva le misure idonee ad evitare la situazione di pericolo.

L'insegnante è responsabile tutto il tempo dell'affidamento dell'alunno alla scuola. Quindi, non soltanto durante le ore delle attività didattiche, ma anche in tutti gli altri momenti della vita scolastica, compresa la ricreazione, la pausa pranzo, la palestra, le uscite e i viaggi di istruzione etc.

L'intervento della scuola è fondamentale per ridurre i rischi e le implicazioni negative, soprattutto in ottica di prevenzione. L'azione della nostra scuola consiste nello sviluppo delle competenze emotive e relazionali degli studenti a livello individuale e di gruppo; l'ambiente scolastico è il contesto ideale per intraprendere azioni di prevenzione mediante la realizzazione di interventi educativi e formativi, finalizzati allo sviluppo armonico della personalità e delle competenze di vita necessarie a relazionarsi positivamente con il mondo. Il nostro Istituto inserirà nel PTOF progetti specifici di azione e intervento adeguati all'età degli alunni. Sin dalla scuola dell'Infanzia la prevenzione avviene sollecitando lo sviluppo di una positiva immagine di sé, il rispetto delle regole, l'educazione ai valori, attraverso la trasversalità e l'interazione dei Campi di esperienza. Nella scuola dell' Infanzia, Primaria e Secondaria di I grado si agisce attraverso l'educazione affettiva, emotiva, relazionale in chiave interdisciplinare; le esperienze, i contenuti e le attività saranno calibrati in base al periodo di crescita e saranno affrontati in modo gradatamente sempre più articolato e complesso, anche con interventi di carattere formativo e disciplinare previsti dal Regolamento di Istituto.

Gli interventi di prevenzione, formazione e presa in carico devono avvenire su diversi livelli: con la comunità scolastica, con il gruppo classe, e con il singolo.

Si prevedono nel corso del triennio:

percorsi di formazione specifica dei docenti;

attività informativa e di sensibilizzazione rivolta a ragazzi, genitori, insegnanti e personale scolastico;

incontri di formazione, incontri/dibattito tenuti da esperti (psicologi, sociologi, Polizia postale, giudici del Tribunale dei minori, referenti associazione genitori, Enti del territorio), per alunni, docenti, genitori al fine di far conoscere il fenomeno delle devianze, gli strumenti di comunicazione/interazione in Internet, i possibili rischi della rete;

interventi a livello di classe che prevedono la partecipazione attiva ed esperienziale degli studenti;

visione di filmati, spot, cortometraggi sul tema; discussione guidata, letture tematiche e debate;

interventi a livello individuale: si agisce direttamente con il bullo e con la vittima, singolarmente. I ragazzi coinvolti necessitano di un'attenzione particolare e di un aiuto psicologico mirato. In questo caso le figure professionali e istituzionali di riferimento possono essere lo psicologo scolastico, i professionisti del

Dipartimento prevenzione territoriale Asur 4, la Polizia Postale.

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.

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete. L'Istituto promuoverà interventi di formazione degli studenti e delle studentesse tenuti dai docenti e da esperti esterni (forze dell'ordine, psicologi, personale sanitario), mirati alla sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme online.

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?

La dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica, che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

La scuola proporrà momenti di riflessione in modo che i ragazzi comprendano che la tecnologia è uno strumento utile per raggiungere i propri obiettivi e non solo distrazione o gioco. Integrando la tecnologia nella didattica, pratica diffusa e collaudata presso l'Istituto, se ne mostra un suo utilizzo funzionale che contribuisce a rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online. L'argomento "benessere digitale" sarà inserito anche nei percorsi di educazione civica e cittadinanza digitale, con l'intento di non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo della rete.

4.5 - Sexting

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

Data l'importanza di questa tematica l'Istituto promuoverà interventi di formazione degli studenti e delle studentesse tenuti dai docenti e da esperti esterni (forze dell'ordine, psicologi, personale sanitario).

4.6 - Adescamento online

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

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità.

Fondamentale quindi, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).

Se si ha sospetto o certezza di un caso di adescamento on line, la scuola provvederà subito ad informare la famiglia e a mettersi in contatto con la Polizia Postale e, poiché si tratta di una problematica molto delicata da gestire, che può avere ripercussioni psicologiche significative sul minore, potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o

psichiatrico.

A scopo preventivo l'Istituto promuoverà interventi di formazione degli studenti e delle studentesse tenuti dai docenti e da esperti esterni (forze dell'ordine, psicologi, personale sanitario, associazioni di volontariato).

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](#).

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. Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio.

Anche relativamente a questa problematica l'Istituto promuoverà interventi di formazione degli studenti e delle studentesse tenuti dai docenti e da esperti esterni (forze dell'ordine, psicologi, personale sanitario, associazioni di volontariato).

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli

studenti/studentesse.

- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/le studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della

diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/le studenti/studentesse.

Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.

Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

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

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/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona 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:1.96.96).

Per quanto riguarda la gestione dei casi, il nostro Istituto ha individuato una figura referente per il cyberbullismo.

La segnalazione del caso dovrà quindi essere fatta dal singolo docente, tramite modulo allegato al presente documento (Scheda di segnalazione), alla referente, la quale, insieme al Team per le emergenze, si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti e di segnalare l'accaduto al Dirigente. Sarà poi il Dirigente, insieme al Team, a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti. Si sceglierà uno o più interventi da attuare a cui seguirà una fase di monitoraggio. (cfr. Diario di bordo)

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.

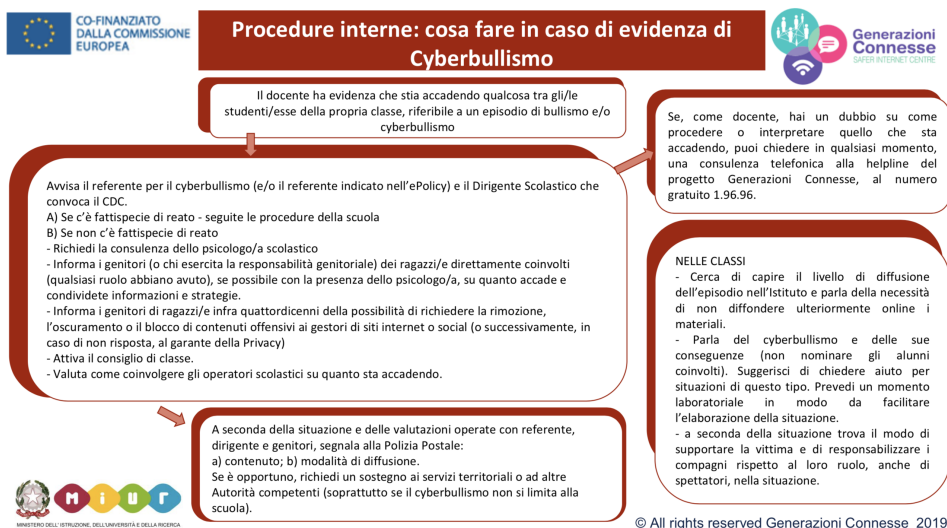
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

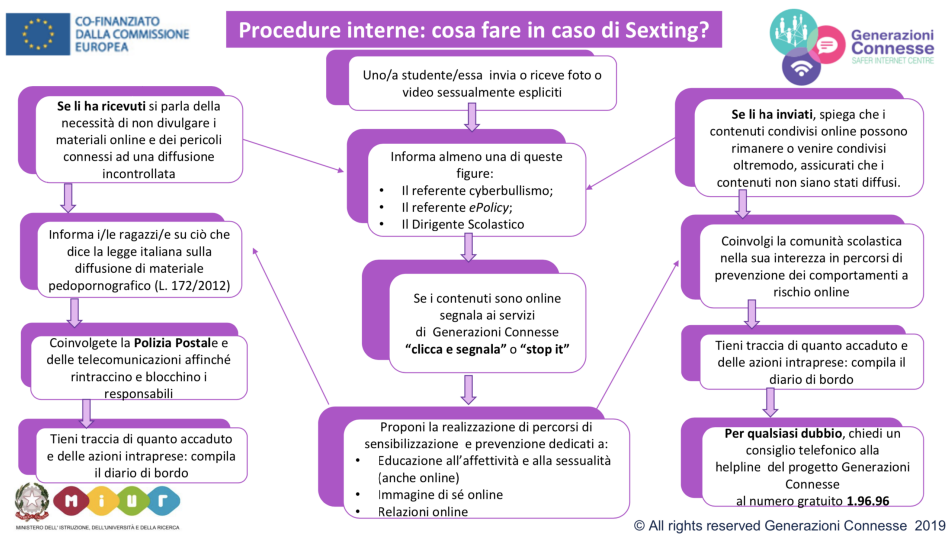
5.4. - Allegati con le procedure

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

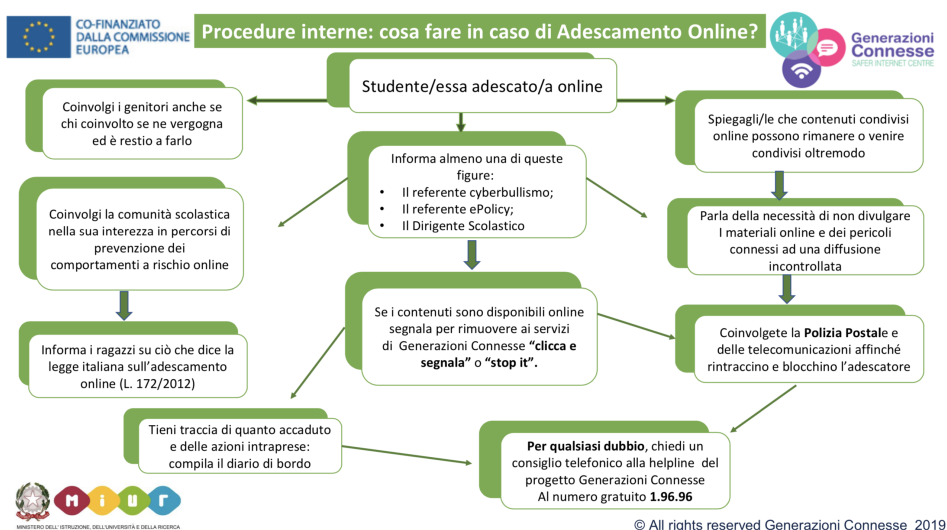




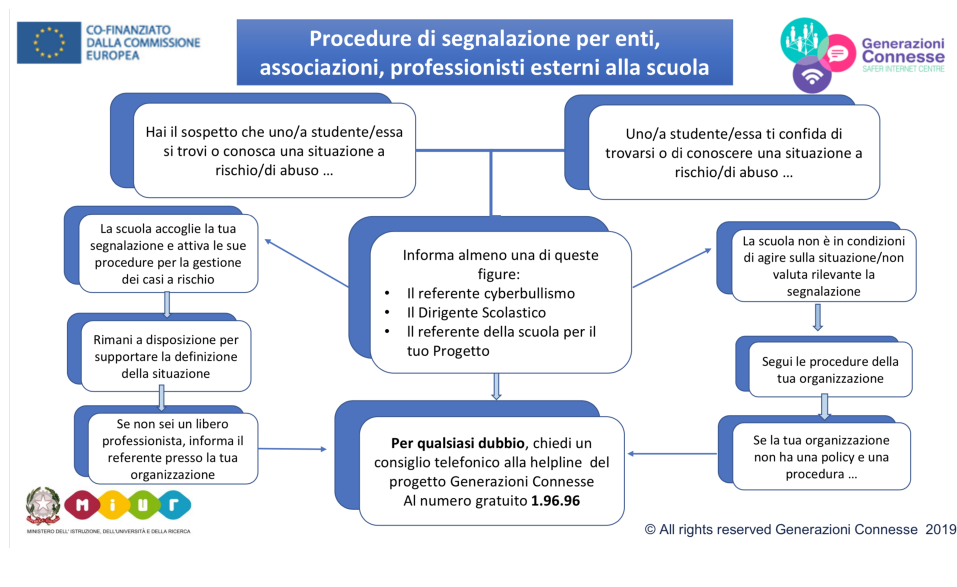
Procedure interne: cosa fare in caso di sexting?



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

Non è prevista nessuna azione.

