



Documento di ePolicy

RMIC8E700Q

IC VIA ACQUARONI

VIA ACQUARONI53 - 00133 - ROMA - ROMA (RM)

Guglielmo Caiazza

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.

Il presente documento ha lo scopo di descrivere le norme comportamentali e le procedure per l'utilizzo delle ICT nell'Istituto Comprensivo "Via Acquaroni" di Roma, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali. La nostra scuola, nello specifico, si impegna a :

1. adottare le misure atte a facilitare e a promuovere l'uso delle ICT nella didattica e negli ambienti scolastici;
2. stabilire le misure di prevenzione e di gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

Grazie a un percorso guidato e al materiale di supporto messo a disposizione sul sito del progetto www.generazioniconnesse.it, si definiscono qui le misure che l'Istituto intende adottare:

- per la promozione dell'utilizzo delle ICT nella didattica;
- per la prevenzione, ovvero le azioni finalizzate alla prevenzione di fenomeni legati ai rischi delle tecnologie digitali;
- per la segnalazione dei casi, ovvero le disposizioni semplici su come segnalare i casi nella scuola;
- per la gestione dei casi, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti che sono stati vittime o spettatori attivi e/o passivi di quanto avvenuto.

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.

Nell'ambito della E- policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

Il Dirigente Scolastico

- garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- garantire ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line;

L'Animatore digitale (come da PNSD)

- Formazione interna - stimolare la formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di laboratori formativi, favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative, come ad esempio quelle organizzate attraverso gli snodi formativi;
- Coinvolgimento della comunità scolastica - favorire la partecipazione e stimolare il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, anche attraverso momenti formativi aperti alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa;
- Creazione di soluzioni innovative - individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; adozione di metodologie comuni; informazione su innovazioni esistenti in altre scuole; laboratorio di robotica educativa e pensiero computazionale), coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure (team dell'innovazione, gruppo SNODO, personale tecnico esterno).

Il Referente bullismo e cyberbullismo

“Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo” (Art. 4 Legge n.71/2017, “Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo”).

- coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio.
- coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori

I Docenti

- provvedere alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri:

lotta al cyberbullismo);

- sviluppare le competenze digitali degli alunni e fare così in modo che conoscano e seguano le norme di sicurezza nell'uso del web e utilizzino correttamente le tecnologie digitali sia a scuola sia nelle attività didattiche extracurricolari;
- segnalare prontamente alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabilire comuni linee di intervento educativo per affrontarle;
- segnalare al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di infrazione.

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

- assicurare, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione richiesti da cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate;
- facilitare la trasmissione di comunicazioni relative alle tecnologie digitali tra le varie componenti della scuola (Dirigente scolastico, Animatore digitale, team dell'innovazione, gruppo SNODO, tecnici esperti esterni, assistenti esterni per il registro elettronico, docenti e famiglie degli alunni);
- curare la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti, provvedendo all'intervento del personale tecnico di assistenza.

DPO (Data Protection Officer)

Figura introdotta dal Regolamento generale sulla protezione dei dati 2016/679 GDPR, è un professionista che deve avere competenze giuridiche, informatiche, di risk management e di analisi dei processi. Nel nostro Istituto il ruolo è affidato alla Infotek s.r.l., i cui compiti sono:

- osservare, valutare, organizzare la gestione del trattamento dei dati personali
- informare e fornire consulenza al Titolare del Trattamento o al Responsabile dello stesso
- sorvegliare l'osservanza del Regolamento Privacy UE 2016/679 (GDPR), di altre Disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo

Gli Studenti e le Studentesse

- ascoltare e seguire le indicazioni fornite dai docenti per un uso corretto e responsabile delle tecnologie digitali, attuando le regole di e-safety per evitare situazioni di rischio;

- chiedere l'intervento dell'insegnante e/o dei genitori nello svolgimento dei compiti a casa per mezzo del digitale, qualora insorgano difficoltà o dubbi nel suo utilizzo.

I Genitori

- contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- incoraggiare l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- agire in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.

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).

Al fine di rendere l'ePolicy uno strumento efficace per la tutela degli studenti e delle studentesse, intesa in senso ampio, sarebbe utile individuare un insieme di regole o

norme di comportamento da condividere con le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve e/o lungo periodo.

I soggetti esterni trovano nell' E-Policy le procedure di segnalazione e di tutela per limitare e contrastare possibili pericoli legati a condotte educative non professionali, finalizzate a rilevare e gestire le problematiche connesse ad un uso non consapevole delle tecnologie digitali.

In questo modo, si faciliterebbe la presa in carico da parte della scuola, qualora si verificassero problematiche derivanti da un utilizzo non corretto delle tecnologie digitali o quando, nei casi più estremi, si sospettassero forme di maltrattamento/abuso sia nel reale che nel virtuale, sia di tipo fisico che psicologico a danno di minori.

È importante garantire che tutti i soggetti esterni che erogano attività in ambito scolastico siano sensibilizzati e resi consapevoli dei rischi online che possono correre gli studenti e le studentesse e dei comportamenti corretti che devono adottare a scuola.

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.

A- Condivisione e comunicazione della Policy agli alunni:

- All'inizio dell'anno scolastico i docenti si occuperanno di illustrare agli alunni, oltre al regolamento d'Istituto, anche questa policy, sottolineando l'importanza educativa insita in essa.
- Nel corso dell'anno saranno dedicate da ciascun docente alcune lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo.

B- Condivisione e comunicazione della Policy al personale:

- Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse in tutti gli organi collegiali e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola.
- Il personale della scuola riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito web dell'Istituto

C- Condivisione e comunicazione della Policy ai genitori:

- Le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola.
- Al fine di sensibilizzare le famiglie sui temi dell'uso delle ICT saranno organizzati dalla scuola incontri informativi, durante i quali si farà riferimento alla presente e-policy.

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.

In relazione a quanto specificato in questa E-policy le infrazioni saranno gestite in modo graduale rispetto alla gravità dell'infrazione e, nel caso degli alunni, anche alla loro età.

Infrazioni degli alunni.

È bene che i docenti introducano, preventivamente, attività laboratoriali miranti a sviluppare nei loro alunni una sempre maggiore consapevolezza dei rischi legati a un uso imprudente e improprio del web e che forniscano loro, ogniqualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori.

I provvedimenti disciplinari da adottare da parte del consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) saranno i seguenti:

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione; divieto temporaneo di prendere parte alla ricreazione e simili);
- nota informativa sul diario ai genitori;
- convocazione dei genitori per un colloquio con l'insegnante;
- convocazione dei genitori per un colloquio con il Dirigente scolastico;
- rimozione temporanea dei diritti di accesso a internet
- presa in custodia del dispositivo
- sospensione con obbligo di frequenza con il coinvolgimento in attività socialmente utili all'Istituzione Scolastica
- allontanamento temporaneo dalle lezioni
- segnalazione alle autorità competenti.

Infrazioni del personale scolastico.

Le infrazioni alla policy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole qui descritte sulla gestione della strumentazione, sia la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni. Nel primo caso la gravità si valuta sull'esposizione al rischio procurata agli alunni, nel secondo caso sul danno per la non tempestiva attivazione delle azioni qui indicate. La gestione delle infrazioni in quest'ambito ricade nella disciplina contrattuale.

Infrazioni dei genitori.

Compito precipuo dei genitori è supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficaci ai principali rischi rappresentati dalla navigazione in internet di utenti molto giovani e spesso poco accorti. Nel caso di infrazione si prevedono interventi, rapportati alla sua gravità, che vanno dalla semplice comunicazione del problema alla convocazione da parte

dell'insegnante di classe/coordinatore o del Dirigente Scolastico.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti, che specificano il contesto di attuazione delle politiche dell'Istituto Comprensivo per un uso efficace e consapevole del digitale nella didattica:

- PTOF, incluso il piano per l'attuazione del PNSD;
 - POF;
 - Pdm e RAV;
 - Regolamento interno d'Istituto;
 - Regolamenti dei laboratori presenti nell'Istituto;
 - Patto di corresponsabilità;
 - Regolamento della DDI.
-

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio dell'implementazione/aggiornamento della Policy avverrà

- alla fine di ogni anno scolastico, contestualmente alle indicazioni di casi rilevati e non preventivamente considerati nell'e-safety;

- all'inizio di ogni anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore digitale e dei collaboratori del Dirigente, anche attraverso la somministrazione ad alunni e personale scolastico di questionari atti a verificare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare attività volte a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione e conoscenza della nuova ePolicy rivolto ai genitori

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione della nuova ePolicy rivolto ai docenti

Capitolo 2 - Formazione e curriculum

2.1. Curricolo 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.

La competenza digitale, inserita tra le otto competenze chiave a livello Europeo, richiama diverse dimensioni in un’ottica che integra la dimensione tecnologica con quella cognitiva ed etica.

- **dimensione tecnologica:** è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana ed evitare automatismi che abbiano conseguenze incerte, attraverso un’adeguata comprensione della “grammatica” dello strumento.
- **dimensione cognitiva:** fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità.

- dimensione etica e sociale: la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

Dall'integrazione di queste dimensioni emerge un concetto di competenza digitale completo, che fa riferimento alla capacità di comprendere e sfruttare l'effettivo potenziale delle tecnologie come costruzione di conoscenza e di promozione della partecipazione e dell'inclusione. La competenza nell'uso consapevole, critico e creativo delle nuove tecnologie diventa quindi una componente fondamentale nell'ottica della Cittadinanza Digitale, trasversale al curriculum scolastico di ogni alunno/studente.

Il nostro Istituto, nell'ambito del PNSD, già da tempo, ha proposto attività laboratoriali interne ed esterne, come la Settimana del Codice, Robotics School, Coding e Pensiero Computazionale, Strumenti per la Cittadinanza Digitale attraverso la piattaforma e-learning di Arête Formazione, fruizione del materiale e di tutti i contenuti presenti sul sito di Generazioni Connesse, uso dei libri di testo in formato digitale, utilizzo di classi virtuali. È stata, inoltre, incrementata la rete wi-fi e ampliata la dotazione di LIM, tablet e notebook. L'istituto ha da tempo intrapreso una politica di BYOD, "porta il tuo dispositivo", per promuovere una didattica basata sull'integrazione di dispositivi personali degli studenti e degli insegnanti con le dotazioni tecnologiche degli spazi scolastici; ha progettato e realizzato un'aula 3.0 e una 2.0 con attività legate ad esse, come laboratori di scrittura creativa e la formazione di un blog. Il nostro istituto ha deciso di avvalersi della piattaforma "Google Workspace For Education" ritenuta idonea a prestare servizi di didattica a distanza dal Ministero dell'Istruzione: per ogni alunno viene attivato un account Google workspace e guidato all'utilizzo dello stesso. La scuola organizza incontri con la Polizia di Stato (nell'ambito del progetto "Scuole Sicure") ed i Carabinieri, per far comprendere i concetti di prevenzione e sicurezza, di bullismo e cyberbullismo e per illustrare le modalità con cui chiedere aiuto se si presentano situazioni di pericolo. E' stato, inoltre, richiesto anche l'intervento della Guardia di Finanza, nell'ambito del progetto di "Educazione alla legalità economica".

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.

Nell'ambito del PNSD il nostro Istituto ha previsto le figure dell'Animatore Digitale e del Team dell'animazione, formati come previsto. Così come i docenti partecipanti all'aggiornamento dello Snodo Formativo.

La formazione del personale è assicurata da iniziative interne, dalla partecipazione alla formazione di Ambito, dall'adesione alle iniziative organizzate dal MIUR nell'ambito del PNSD.

Il percorso prevede:

- incontri di formazione all'utilizzo del registro elettronico
- corsi on-line
- momenti di auto-aggiornamento
- momenti di formazione personale e/o collettiva organizzati dall'AD, Team e Snodo
- partecipazione a iniziative promosse dalle scuole in rete di ambito o dal MIUR
- visione e fruizione di materiali messi a disposizione sul sito della scuola, riguardanti l'utilizzo e l'integrazione delle TIC nella didattica
- monitoraggio del gradimento e dei risultati conseguiti

E' fondamentale l'utilizzo delle TIC nella didattica: un loro utilizzo strutturato e integrato non solo rende gli apprendimenti motivanti, coinvolgenti ed inclusivi, ma permette al docente di guidare studenti e studentesse rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento al di fuori della scuola.

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

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

L'Istituto programma azioni come:

1. Analisi del fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;
2. Promozione della partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse";
3. Organizzazione di incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.

L'avvio del progetto "Generazioni connesse" ha rappresentato una reale opportunità di rendere coesa e unitaria la formazione on-line dei docenti sull'uso consapevole e sicuro della rete e delle tecnologie digitali. Si è predisposto da alcuni anni nel sito web dell'Istituto uno spazio denominato "Legalità, bullismo e cyberbullismo", in cui i docenti possono trovare materiale informativo sull'argomento, guide in pdf, manuali e link utili all'autoaggiornamento, oltre ai corsi tematici online messi a disposizione dalla piattaforma "Generazioni connesse". Tale sezione sarà ampliata.

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

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

Il nostro Istituto Comprensivo dall'anno scolastico 2017/2018 ha aperto uno sportello di ascolto gestito da uno psicologo, nell'ambito del progetto "Camminiamo insieme...". Lo sportello risponde a richieste di consulenza di alunni della scuola primaria, distudenti della scuola superiore di 1 grado, di genitori e docenti, inerenti a tematiche di difficoltà/disagio reazionale e sospetti episodi di bullismo e cyberbullismo. Ha attuato, inoltre, nella scuola primaria dei laboratori esperienziali rivolti a tutte le classi. Data l'affluenza elevata, come previsto dalla precedente epolicy, la presenza a scuola è stata incentivata.

Il corpo docente, dopo l'aggiornamento dell'E-Safety Policy d'Istituto, si propone di attuare le seguenti azioni :

- Comunicazione e presentazione ai genitori del Regolamento della Policy
- Fornire periodicamente leaflet informativi sull'argomento
- Fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito www.generazioniconnesse.it e Telefono Azzurro
- Informare e formare sull'uso consapevole della rete e sui pericoli derivanti da una scarsa conoscenza della stessa in occasione di incontri scuola-genitori per condividere con essi regole comuni.

L'Istituto informa le famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'e-Policy e dal suo piano di azioni, anche attraverso l'aggiornamento del Regolamento scolastico, del "Patto di corresponsabilità" e del nuovo Regolamento della Didattica Digitale Integrata. Nella sezione dedicata sul sito web dell'Istituto saranno presenti consigli ai genitori su come gestire la relazione dei propri figli con le tecnologie digitali, in particolare nella comunicazione con i figli e in generale in famiglia, facendo riferimento anche alla sezione dedicata ai genitori del sito www.generazioniconnesse.it

Il nostro piano d'azioni

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

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.

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

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- 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.

Per la protezione dei dati personali, il principale riferimento normativo è attualmente la Carta dei Diritti fondamentali dell'Unione Europea (art 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 2016. Tuttavia, si possono individuare al riguardo alcune linee guida di e-safety.

All'interno dell'istituzione scolastica, il responsabile della gestione del trattamento dei dati personali è il Dirigente Scolastico, il quale indica nella persona del DSGA e nel personale amministrativo gli incaricati al trattamento di tali dati.

Il suddetto personale è istruito sulla procedura da seguire per segnalare eventuali incidenti in cui la protezione dei dati potrebbe essere stata compromessa, ad usare sistemi di logout al momento di lasciare i computer utilizzati e ad impostare il logout (bloccaggio) dopo un certo periodo di inattività.

La segreteria utilizza password nelle postazioni informatiche di lavoro, individua soggetti preposti alla gestione delle password, ha un codice identificativo personale per ogni utente, utilizza programmi antivirus, protegge e regola gli accessi locali che ospitano i dati riservati o in cui si trovano le postazioni di lavoro che ne consentono l'accesso, definisce i criteri per garantire l'integrità e la trasmissione sicura dei dati e si dota di mezzi elettronici adeguati per impedire l'accesso dall'esterno alla propria rete.

Lo smaltimento di qualsiasi apparecchiatura deve essere conforme alle norme di smaltimento dei rifiuti elettrici ed elettronici e per qualsiasi server contenente dati personali o soggetti alla tutela della privacy è necessario un certificato di cancellazione sicura.

Il personale della scuola può condividere numeri di telefono personali con la componente studentesca e genitoriale solo in casi limitati relativi a scopi didattici e organizzativi, mentre gli indirizzi di posta elettronica istituzionali dei docenti permettono uno scambio regolato e regolare. Per la costante e quotidiana comunicazione con la componente studentesca-famiglia è attivo un numero telefonico per ogni plesso dell'Istituto e un indirizzo e-mail, entrambi presenti sul sito istituzionale.

Le fotografie o i video da pubblicare sul sito che includano alunni e alunne saranno selezionati con cura e non permetteranno l'identificazione dei singoli attraverso l'indicazione del nome, a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. Si preferirà l'utilizzo di fotografie o video di gruppo. All'atto dell'iscrizione, è richiesto alle famiglie di firmare

un'autorizzazione per consentire l'uso didattico di immagini e video dei minori secondo i principi sopra indicati. Ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che avrà valore solo per lo specifico evento.

La nostra scuola ha l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato ormai in vigore. In esso sono indicate le linee guida da seguire riguardo il trattamento dei dati personali all'interno della comunità scolastica. Tutte le scuole hanno l'obbligo di far conoscere agli studenti, alle famiglie e ai docenti le modalità di trattamento dei loro 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 studenti. Alcune categorie di dati personali degli studenti e delle famiglie, come quelli sensibili e giudiziari, devono essere trattate nel rispetto di specifiche norme di legge, verificando prima non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle finalità di rilevante interesse pubblico che si intendono perseguire.

Ogni persona ha diritto di conoscere se sono conservate informazioni che la riguardano, di apprenderne il contenuto, di farle rettificare se erranee, incomplete o non aggiornate. Per esercitare questi diritti è possibile rivolgersi direttamente al "titolare del trattamento", anche tramite i suoi incaricati o responsabili del trattamento dei dati. Se non si ottiene risposta o se il riscontro non risulta adeguato, è possibile rivolgersi al Garante o alla magistratura ordinaria.

L'accesso agli atti amministrativi è regolato dalla singola amministrazione che deve valutare l'esistenza di presupposti normativi che permettono di prendere visione e di estrarre copia dei documenti amministrativi ai soggetti con un "interesse diretto, concreto e attuale" alla conoscibilità degli atti.

Le istituzioni scolastiche devono prestare particolare attenzione a non diffondere, anche per mero errore materiale, dati idonei a rivelare lo stato di salute degli studenti, così da non incorrere in sanzioni amministrative o penali.

L'utilizzo di telefoni cellulari e di apparecchi per la registrazione di suoni e immagini è disciplinato dal Regolamento di Istituto pubblicato sul sito della scuola. Tuttavia nessun membro della comunità scolastica, in alcuna occasione (ad esempio, all'interno della scuola o durante un'uscita didattica), può diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso.

Le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici non violano la privacy. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione. Va, però, prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini

su Internet. In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video o dei genitori (o di chi ne fa le veci) nel caso di minori.

Le scuole di ogni ordine e grado sono soggette a un regime di pubblicità e trasparenza. È però necessario che gli istituti scolastici prestino particolare attenzione a non rendere accessibili informazioni che dovrebbero restare riservate o a mantenerle online oltre il tempo consentito, mettendo in questo modo a rischio la privacy e la dignità delle persone a causa di un'errata interpretazione della normativa o per semplice distrazione.

3.2 - Accesso ad Internet

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

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

Internet” diventi una realtà, a partire dalla scuola”.

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

La scuola è presente sulla rete con un portale web costantemente aggiornato contenente informazioni utili per il personale scolastico e per le famiglie. Il sito a seguito della determina n.36 del 12 febbraio 2018, è stato fatto migrare da suffisso gov.it a suffisso edu.it. L’utilizzo del protocollo https protegge l’integrità e la riservatezza dei dati scambiati online protetto da un protocollo di trasmissione dei dati sicuro (https) all’aggiornamento di software e sistemi operativi.

L’I.C. è dotato di una connessione web tramite fibra ottica che serve tutti i plessi di scuola primaria e secondaria di primo grado. Attualmente la scuola dell’infanzia non è ancora coperta da connessione internet, ma grazie ai fondi del Pon si provvederà entro il termine del corrente anno scolastico a dotare i plessi della copertura necessaria.

L’accesso ad internet è consentito esclusivamente per scopi educativi e didattici. I plessi della scuola primaria e secondaria sono dotati di laboratori d’informatica i cui computer sono interconnessi tramite un sistema di rete Lan. I laboratori della scuola primaria e secondaria sono sufficientemente attrezzati sia con strumenti fissi che con strumenti mobili e vengono monitorati per garantire l’efficienza dalle Funzioni Strumentali e da un assistente tecnico. L’Istituto è dotato di un laboratorio 3.0, situato nel plesso di Via Merlini, con Lim, tablet e televisore touch in cui è possibile strutturare lezioni interamente a carattere digitale o lezioni tradizionali che possono venire integrate dal digitale.

Tutte le classi della primaria e della secondaria sono dotate di un notebook con cui i docenti possono raggiungere il registro elettronico di classe e utilizzare il proprio account Google per creare, modificare e condividere documenti con alunni e colleghi. Molte classi della scuola primaria sono dotate di Lim, almeno una per ogni gruppo di classi parallele. Essendo risultati vincitori del progetto Pon Digital Board, in ogni classe verrà installata un panel touch, mentre le Lim esistenti saranno posizionate in supporto dei laboratori nelle scuole dell’infanzia. Nessun dispositivo presente nell’Istituto è protetto da antivirus, poiché i documenti vengono utilizzati e condivisi solo tramite account di Google che ne garantisce la sicurezza. I servizi di manutenzione e di assistenza informatica sono gestiti dalla società Infotek srl che assolve in tempi consoni alle segnalazioni.

La criticità da affrontare a breve è quella di munire ogni classe di un punto Lan per limitare l’inquinamento da onde elettromagnetiche. Inoltre, per garantire la sicurezza durante la navigazione Internet nelle parti in cui verrà mantenuta la connessione wifi, sarà necessario intervenire per la messa in sicurezza dei dati sensibili tramite firewall.

Gestione accessi (password, backup, ecc.)

L’accesso al sistema informatico per la didattica, server e internet, nel laboratorio multimediale e nelle aule è consentito al personale docente attraverso l’utilizzo del

nome utente della scuola e password univoci. Per ciò che riguarda l'uso dei laboratori, i docenti registrano il proprio accesso scrivendo negli appositi registri la data, l'orario di utilizzo dei laboratori ed eventuali annotazioni su riscontri di malfunzionamenti della strumentazione. Non vi è un backup dei file elaborati, se non quello operato dai docenti interessati sul proprio drive. Ciclicamente i responsabili di laboratorio effettuano una pulizia

dei device. Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi. Ogni pc è dotato di un doppio account: uno protetto da una password conosciuta solo dai docenti responsabili, uno privo di pw, utilizzabile solo come fruitori.

Al di fuori del laboratorio ogni classe ha a disposizione un suo notebook, così come quasi tutti i laboratori della scuola. Tutti questi dispositivi sono protetti da password conosciute solo dai docenti.

Inoltre, la scuola ha a disposizione numerosi tablet acquistati in seguito all'emergenza sanitaria ancora in corso. Questi dispositivi vengono dati in comodato d'uso alle famiglie in caso di didattica a distanza. Ogni dispositivo funziona tramite un account della scuola, ma ogni famiglia, nel periodo di utilizzo, installa l'account personale dell'alunno per l'accesso a Classroom. I docenti della Commissione Digitale si occupano di ripulire e controllare i tablet alla loro riconsegna.

E-mail

L'account di posta elettronica dei docenti è solo quello istituzionale ed è utilizzato unicamente per comunicazioni, in entrata e in uscita, di carattere lavorativo. Gli utenti si impegnano a non diffondere informazioni che possono nuocere alla reputazione della scuola o essere contrarie alla morale o alle leggi in vigore.

Ogni docente è dotato di un proprio account Gmail col dominio della scuola collegato all'account .edu.it. La mail di questo account è diventato il riferimento per le comunicazioni ufficiali.

Blog e sito web della scuola

Il Sito web della scuola è il punto di riferimento per tutti gli aggiornamenti sui progetti. La scuola attualmente è dotata di un sito istituzionale con estensione "edu.it". Esso è stato lanciato nell'a.s. 2015/16 da un web master esterno (Infotek S.a.s.), utilizzando i contenuti e le pagine create e lanciate precedentemente dall'attuale Animatore Digitale. Il web master ha cura di effettuare aggiornamenti e backup periodici e interviene in caso di emergenza.

Sul sito web sono presenti:

1. L'indirizzo della scuola, e-mail e numero di telefono.
2. Le varie pagine, compresa la home del sito, vengono aggiornate quasi quotidianamente dall'Animatore Digitale, che ne valuta, con il Dirigente Scolastico, la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, nel rispetto della privacy.
3. L'area relativa alle circolari è gestita ed aggiornata dal personale di Segreteria, individuato ed incaricato per specifiche competenze tecnico-informatiche.

Il sito prevede un' area pubblica, per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica,

le iniziative, le scadenze ministeriali, avvisi di carattere generale, e delle aree riservate, accessibili solo dopo autenticazione con password diversificate:

- o per i docenti e il personale ATA: che possono visualizzare le circolari e la modulistica.

- o per i membri del consiglio d'Istituto: che possono visualizzare verbali o piani annuali non ancora deliberati.

- o per il MIUR: che può visionare materiale strettamente riservato non pubblico.

Tra i contenuti pubblici, accessibili ai visitatori e suddivisi per argomenti, è possibile trovare regolamenti, materiali didattici, pubblicizzazione di eventi, documentazione di attività curriculari ed extracurriculari svolte e la bacheca sindacale (RSU). Nell'area "presentazione dell'Istituto" ogni anno vengono realizzati e caricati materiali digitali rappresentativi dei progetti svolti nei tre ordini di scuola. Le fotografie e i video pubblicati includono allieve e allievi le cui famiglie hanno concesso opportuna autorizzazione. All'atto dell'iscrizione infatti è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video delle/dei minori finalizzati all'attività didattica secondo i principi sopra indicati. L'Animatore Digitale ha inoltre predisposto banner (pulsanti) attivi che permettono l'accesso a link di interesse tra cui quello di "Classeviva" (registro elettronico, le credenziali di accesso vengono fornite alle famiglie all'inizio del primo anno scolastico nell'Istituto), "Programma il Futuro" (per diffondere concetti di base dell'informatica attraverso la programmazione coding), "Generazioni Connesse" (per la prevenzione e il contrasto al bullismo e al cyberbullismo a scuola), "Scuola in chiaro" (per cercare le scuole, esaminare e confrontare le caratteristiche), MAD, Legalità e bullismo, PON, Trinity, Dele, materiale inclusione. Il sito web dell'Istituto offre, inoltre, altri servizi alle famiglie ed agli utenti esterni, quali consultazione del PTOF; Sportello di ascolto; Biblioteca scolastica multimediale; Regolamento d'Istituto; Albo on line; Amministrazione trasparente; Servizio mensa (con i menu diversificati per la sezione primavera/ponte, scuola dell'infanzia, scuola primaria e secondaria di primo grado); ed altre informazioni generali sulla scuola.

Tra i progetti futuri è contemplata la possibilità di aggiungere Blog per ogni classe a scopo didattico collaborativo che sarà utilizzato per scambio di informazioni e materiale.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente

interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

L'Istituto Comprensivo Statale Via Acquaroni ha attivato la piattaforma "G-Suite for Education" sul proprio dominio istitutocomprensivoacquaroni.edu.it per offrire ai propri studenti la possibilità di usufruire di nuovi e stimolanti metodi di apprendimento, coerenti con il Piano Nazionale Scuola Digitale ed altresì con le odierne forme di comunicazione e sviluppo delle conoscenze supportate dalla tecnologia informatica. Per queste ragioni la piattaforma è attualmente la più utilizzata nelle scuole italiane e il suo impiego è fortemente sostenuto dal MIUR.

"G-Suite for Education" è un sistema ad accesso limitato e protetto che non consente la libera registrazione: per accedere alla piattaforma è necessario essere registrato da parte dei suoi amministratori. Questa modalità di partecipazione assicura un buon livello di controllo degli accessi e delle operazioni svolte dagli utenti sul cloud, nonché un ottimo controllo della privacy. G-Suite include decine di funzioni di sicurezza progettate specificatamente per mantenere i dati al sicuro, protetti e sotto controllo. I dati appartengono solo agli utenti e gli strumenti di G Suite consentono loro di controllarli e di stabilire con chi e in che modo dividerli.

L'Istituto ha intenzione di fornire anche al personale ATA degli account personali di modo che possano essere sfruttate appieno le potenzialità della piattaforma.

La piattaforma G Suite for Education non include annunci promozionali, non utilizza mai i contenuti o i dati degli studenti a fini pubblicitari. Essa inoltre ha un valore fortemente inclusivo, in quanto consente agli studenti di imparare a lavorare in modo collaborativo e condiviso.

Per poter accedere al servizio gli studenti utilizzano un account scolastico gratuito con nome utente e password, che potrà essere utilizzato dagli stessi fino al termine del loro percorso all'interno dell'Istituto con la supervisione degli insegnanti e genitori. Si sottolinea che docenti, amministratori e personale di segreteria non hanno accesso ai dati di login degli utenti, né sono in grado di visualizzare alcun tipo di informazione personale.

Sarà cura della famiglia, qualora non volesse che il proprio figlio appaia in video-conferenza con i docenti, disattivare la webcam. Allo scopo di aumentare ulteriormente il livello di sicurezza e di privacy degli account personali, occorre modificare la password iniziale fornita dall'Istituto in fase di attivazione dell'account. Si ricorda che, essendo l'account strettamente personale, la password non potrà essere ceduta a terzi e dovrà essere accuratamente conservata. Qualora fosse smarrita, è comunque possibile recuperarla mandando una mail aadmin@istitutocomprensivoacquaroni.edu.it.

La piattaforma sarà operativa secondo un calendario che ogni consiglio di classe/interclasse comunicherà via mail ai propri alunni. È possibile utilizzare pc fissi, portatili, tablet o smartphone accedendo direttamente a G-suite oppure scaricare l'applicazione Hangouts Meet e Classroom da Google Play o App Store.

La piattaforma è operativa in via sperimentale a partire da maggio 2020. Si precisa che il Regolamento d'Istituto è stato integrato con il Regolamento della Didattica

Digitale Integrata che ha approvato l'utilizzo della piattaforma in questione.

Oltre a "Gsuite for Education" i docenti possono usufruire del Registro elettronico ClasseViva che fa parte della suite Infoschool di Spaggiari, che comprende registro di attività extracurricolari, aule virtuali e Scrutinio online. Tra le varie funzionalità, ClasseViva consente di gestire il Giornale del professore, l'Agenda di classe, le valutazioni, le note e le sanzioni disciplinari, la Bacheca delle comunicazioni e i colloqui scuola-famiglia.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle 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.

L'uso dei dispositivi personali, durante la didattica, non è consentito per gli studenti. Solo durante le uscite didattiche e i campi scuola, gli alunni sono autorizzati dai docenti con tempi e modalità di utilizzo, secondo il Regolamento d'Istituto.

I docenti sono autorizzati ad utilizzare dispositivi personali solo per attività didattiche e legate alle attività funzionali all'insegnamento.

Il nostro piano d'azioni

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

- Copertura LAN, dove è possibile, per ridurre inquinamento elettromagnetico
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

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

- 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.

Il telefono cellulare o lo smartphone non sono richiesti dal nostro Istituto, perché non sono ritenuti indispensabili in ambito scolastico, ma vengono forniti dai genitori degli studenti della Scuola Secondaria di Primo Grado soprattutto per mantenere la comunicazione diretta con i figli fuori dal contesto scolastico. Eludendo la sorveglianza degli insegnanti, attraverso i telefoni cellulari o gli smartphone, dotati di particolari

applicazioni e di collegamento a internet, oltre che parlare e scrivere messaggi con i genitori, gli alunni potrebbero anche scaricare e spedire foto personali o intime, proprie o di altri, video con contenuti indecenti o violenti, accedere a internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi. Eludendo sempre la vigilanza degli insegnanti, gli alunni potrebbero correre gli stessi rischi a scuola anche con l'utilizzo dei pc del laboratorio informatico e con un accesso non controllato a internet.

Se da un lato Internet favorisce la libertà di espressione, dall'altra, purtroppo, gli alunni possono farne un uso scorretto, utilizzando il mondo virtuale come ambiente dove mettere in atto atteggiamenti di violenza e prevaricazione. E' in questo senso che la prevenzione si muove.

Da svariati anni, infatti, il nostro Istituto programma lezioni di Cittadinanza digitale ad opera dell'Animatore Digitale, Referente per il contrasto al bullismo e al cyberbullismo, Referente Legalità, Team dell'Innovazione Digitale e Snodo Formativo. Tali lezioni coinvolgono tutti e tre gli ordini di scuola e mirano non solo a rendere consapevoli alunni/studenti dei rischi della rete e a difendersi perciò da essi, ma anche a sensibilizzarli al rispetto reciproco, alla fattiva collaborazione e all'accettazione della diversità, essenziali per un'inclusione efficace e il superamento degli individualismi.

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 fenomeno del cyberbullismo ha raggiunto dimensioni così allarmanti che una legge dello Stato ha recentemente stabilito precise disposizioni a tutela dei minori per prevenirlo e contrastarlo (n. 71/29-05-2017), nonché un recente aggiornamento (D. M. 18 del 13 gennaio 2021 emanato con nota 482 del 18 febbraio 2021).

Proprio in ottemperanza a tale disposizione legislativa, l'Istituto ha individuato una Referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo. La prima responsabilità del personale della scuola, in primis gli insegnanti, consiste, dunque, nell'imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tali azioni sono spesso sottovalutate dagli alunni, nonostante la competenza tecnica posseduta. Per arginare il fenomeno del bullismo e del cyber-bullismo occorre soprattutto "gestire", attraverso la sensibilizzazione, le dinamiche devianti di gruppo. In esso gli attori sono tre: il bullo, la vittima e il gruppo. Il gruppo ricopre sempre un ruolo fondamentale perché, anche se in modo passivo o inconsapevole, supporta l'azione del bullo. Nel cyber-bullismo, anche un "mi piace" o un "condividi" definiscono la posizione del gruppo, in quanto amplificano la portata della violenza nei confronti della vittima. Occorre quindi prestare particolare riguardo alle implicazioni dei comportamenti "pericolosi" attivati o subiti quali:

- Ø Sopraffazione fisica, verbale e/o psicologica;
- Ø Umiliazione;
- Ø Discriminazione;

Ø Aggressività, violenza, molestia attivata o subita;

Ø Isolamento sociale.

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

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

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

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

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

Il fenomeno di "incitamento all'odio" o "discorso d'odio" (hate speech) è sempre più presente nelle nostre società e ha acquisito particolare visibilità ed estensione dei social network.

Un discorso di incitamento all'odio è una comunicazione con elementi verbali e non verbali mirati a esprimere e diffondere odio e intolleranza, o a incitare al pregiudizio e alla paura verso un individuo o un gruppo di individui accomunati da etnia, orientamento sessuale o religioso, disabilità, altra appartenenza sociale o culturale.

Le buone pratiche per contrastare l'hate speech sono tendenzialmente tre:

1. l'educazione civica digitale, ad esempio veicolare discorsi pacati, non rispondere alle provocazioni;
2. uso del diritto più intelligente che vada a colpire i comportamenti più

esasperati ma salvando la libertà di manifestazione del pensiero;

3. uso intelligente delle tecnologie, magari rendendo più rapide le modalità di segnalazione da parte degli utenti, rendendo efficaci alcuni blocchi o alcune rimozioni di gruppi estremisti, cioè usare anche la tecnologia per cercare di controllare l'odio.

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 rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti, affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

La dipendenza patologica da videogiochi è stata inclusa nella più recente versione del DSM-5. Nello specifico la troviamo sotto l'etichetta "Internet Addiction Disorder", che fa riferimento alle conseguenze negative derivanti da qualsiasi attività che può essere svolta online. Da diversi anni, ormai, gli studi mostrano come la dipendenza da giochi online sia associata a gravi conseguenze per la salute psicofisica della persona:

- drastica riduzione delle relazioni interpersonali;
- riduzione-assenza di hobbies;
- calo nelle abilità attentive;
- aumento dell'aggressività e ostilità;
- aumento dello stress;

Da un punto di vista delle relazioni interpersonali, chi soffre di dipendenza da giochi online preferisce passare il suo tempo con gli amici conosciuti in rete e crede che queste relazioni siano molte più vere e intense rispetto a quelle della vita reale.

La scuola in questo caso ha la possibilità di fare formazione e di indicare strategie per un uso più consapevole delle tecnologie per favorire il

"benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia, tecnologia che i lockdown hanno reso sempre più invasiva. A questo scopo le attività di digital wellbeing programmate dal nostro Istituto sono volte ad un' analisi dello status quo e ad una successiva e consapevole modifica delle abitudini digitali: come trascorro il mio tempo online? quanto trascorro del mio tempo online? cosa cambierei delle mie abitudini online?

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 medialti sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Il termine Sexting, derivato dalla fusione delle parole inglesi sex (sesso) e texting (inviare messaggi elettronici,) è un neologismo per indicare l'invio di messaggi, testi e o immagini sessualmente espliciti, principalmente tramite il telefono cellulare o attraverso canali come chat, social network e varie app.

Il sexting può essere suddiviso:

- scambio di immagini e testi solamente tra due partner.
- scambi di immagini e testi che non coinvolgono solo i due partner ma sono condivisi con altri soggetti estranei alla relazione.
- scambi di immagini e testi tra soggetti che non intrattengono una relazione.

Il sexting nei minori può essere vissuto quindi come una dimostrazione di amore e fiducia nei confronti del proprio partner, come un divertimento o come un modo per sentirsi grandi sia agli occhi degli altri sia di fronte a sè stessi. Questo perchè, rispetto ad altri contesti, attraverso le tecnologie gli adolescenti si sentono più liberi di sperimentare e resta più semplice mettersi in gioco anche con meno pudore.

Le principali conseguenze sono due:

- quelle del web, ovvero quando si perde il controllo delle immagini prodotte, la loro diffusione su web e social network è difficilmente

gestibile. E' bene precisare che in questo caso non si parla più di sexting, ma di "reveng porn"(quando le immagini vengono ad esempio utilizzate da un ex partner a scopi vendicativi e con l'obiettivo di ledere la reputazione della persona ritratta) o di "sextortion" e cyberbullismo (cioè la minaccia di diffusione del materiale foto/video, sempre con l'obiettivo di ledere la reputazione della persona ritratta).

- quelle emotive,

Queste riguardano l'affettività, e in particolare il tema del consenso. La pressione dei pari ("lo fanno tutti o tutte"), ricatti o minacce ("se non lo fai, non mi ami"), i problemi di autostima o il sentirsi in dovere nei confronti del proprio partner al fine di evitare il senso di colpa, possono essere tutti elementi che portano un ragazzo o una ragazza a cedere a comportamenti che non rispettano i suoi tempi o desideri.

4.6 - Adescamento online

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

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

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

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

Il processo di adescamento avviene in cinque fasi, ma quella iniziale dell'amicizia, che comporta un avvicinamento alla vittima, è quello che può metter fine al processo ed anche quello più delicato. I minori vittime riferiscono, generalmente, di sentirsi traditi

e nello stesso tempo di provare un senso di colpa per essere caduti in trappola ed essersi fidati di un estraneo. L'adescamento, inoltre, può essere una problematica molto delicata da gestire e avere ripercussioni psicologiche significative sul minore. Aiutare ragazzi e adolescenti a proteggersi dal web," scegliendo con cura chi frequentare online, è quindi un compito importante degli adulti che li circondano, a partire da genitori e insegnanti, per tutelarli nella vita reale. Il nostro Istituto ha implementato negli ultimi anni, come prefissato nella precedente esafety, lo Sportello d'ascolto per un percorso di educazione (anche digitale) all'affettività e alla sessualità. Lo psicologo, presente nell'Istituto come figure nota di riferimento, ha messo in grado gli alunni/studenti di sapere a chi rivolgersi in caso di situazioni come queste o quelle che si espliciteranno nel paragrafo seguente, anche quando perciò si vergognano, pensano di aver fatto un errore e temono di essere giudicati e non ascoltati. Il nostro personale docente si sta formando sempre più sul tema dell'affettività e della sessualità, affrontando queste tematiche con gli alunni/ studenti, affinché nella solitudine dei loro dispositivi, essi non "formino" una sessualità distorta (uomo forte, donna oggetto).

Per consigli e supporto è previsto rivolgersi alla [Helpline di Generazioni Connesse \(19696\)](#), dove gli operatori esperti e preparati sono sempre a disposizione del personale scolastico oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

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](#).

La pedopornografia è un reato che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini, bambine e adolescenti coinvolti in comportamenti sessualmente espliciti, reali o simulati e qualsiasi rappresentazione degli organi sessuali di persone minorenni a fini soprattutto sessuali. Durante il periodo di emergenza coronavirus si sono ampliati i fattori che espongono alla pedopornografia online. Tra questi: l'aumento della vulnerabilità, la diminuzione della supervisione genitoriale, la mancanza di rete extra familiari, l'aumento della fruizione di ambienti online, l'aumento di contenuti sessuali autoprodotti e scambiati.

Le immagini e i video pedopornografici sono la registrazione visiva della violenza sessuale commessa su un bambino, una bambina o un adolescente. Segnalare la presenza di materiale pedopornografico online, consente alle forze dell'ordine di investigare non solo chi produce, detiene e condivide questo materiale ma, soprattutto,

di identificare i minori presenti nelle immagini e nei video e assicurare loro la protezione e il supporto necessari.

Va sottolineato che il fenomeno della pedopornografia online è per sua natura transnazionale e la lotta alla diffusione implica coinvolgimento di molteplici attori, principalmente le Forze dell'Ordine locali e internazionali, istituzioni e i servizi sul territorio.

Navigando in Rete se si incontrasse materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito "www.generazioniconnesse.it" alla sezione Segnala. Questo per facilitare il processo di rimozione del materiale dalla Rete e allo stesso tempo consentire alle attività investigative ad identificare chi possiede il materiale, chi lo diffonde e chi lo produce, ma soprattutto identificare i minori abusati assicurando la fine di un abuso.

Il nostro piano d'azioni

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

- ☐ Organizzare un incontro informativo 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 laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.

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

- ☐ 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 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.

☐ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

segnalare la presenza di materiale pedopornografico online.

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile dei social network.

I docenti segnaleranno comportamenti inconsueti e inadeguati degli alunni, fatti riferiti dagli alunni e/o dalle famiglie ai docenti; contenuti pericolosi inviati o ricevuti da altri, messi o scaricati in rete dagli alunni.

In particolare si segnaleranno:

Ø contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, informazioni false, ecc.);

Ø contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, siti d'odio, insulti, ecc...);

Ø contenuti afferenti alla sessualità (messaggi molesti, conversazioni di testo o voce riguardanti la sessualità, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali, ecc...).

Tutte le segnalazioni riportate dai docenti verranno registrate su apposita scheda messa a disposizione dal sito www.generazioniconnesse.it

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).

Lo Sportello d'ascolto, attivo nel nostro Istituto, ha la funzione di raccogliere segnalazioni anonime da poter riporre in apposite scatole situate presso le portinerie dei plessi, oltre a fornire l'assistenza dello psicologo.

Per le segnalazioni di fatti rilevati sono previsti i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto:

- Ø annotazione del comportamento sul registro elettronico in uso, con notifica di lettura della famiglia
- Ø comunicazione scritta ai genitori, che la devono restituire vistata;
- Ø convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;
- Ø relazione scritta al Dirigente scolastico.

La legge rimette ai genitori dell'alunno la scelta di richiedere l'ammonizione del colpevole attraverso la querela, per quanto riguarda i reati meno gravi.

Per i reati più gravi, i docenti hanno l'obbligo di allertare le autorità competenti e di presentare la denuncia qualora se ne avvisino gli estremi di reato.

Nella denuncia dovrà essere esplicitato:

- Ø il fatto e il giorno dell'acquisizione del fatto;
- Ø le fonti di prova;
- Ø le generalità e il domicilio della persona a cui è attribuito il reato;
- Ø la persona offesa;
- Ø i testimoni.

A chi bisogna segnalare:

- Ø Ai genitori;
- Ø Al Dirigente Scolastico;
- Ø Al Referente del bullismo e cyberbullismo;
- Ø Ai docenti;
- Ø Allo psicologo dello Sportello di ascolto dell'I.C.;
- Ø Alla helpline di Generazioni Connesse, al numero gratuito 1.96.96.;
- Ø Alla Polizia postale.

Inoltre, ci si potrà avvalere dei due servizi messi a disposizione dal Safer Internet Center: il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children. Una volta ricevuta la segnalazione, infatti, gli operatori procederanno a coinvolgere le autorità competenti in materia.

Come gestire le segnalazioni.

Il docente venuto a conoscenza del fatto dovrà:

- Ø Informare tempestivamente il Dirigente Scolastico;
- Ø Informare tempestivamente la Referente del bullismo e cyberbullismo tramite modulo;
- Ø Informare tempestivamente il Coordinatore di classe e il Consiglio di Classe dell'alunno oggetto di cyberbullismo;

- Ø Informare i genitori dell'alunno oggetto di cyberbullismo, offrendo loro la possibilità di avere il supporto dello psicologo della scuola per affrontare al meglio la situazione;
- Ø La Referente, in collaborazione con il C.d.c. o team docenti, raccoglierà tutte le informazioni possibili;
- Ø Il C.d.c. o team docenti valuterà, a seconda della gravità del caso, come sanzionare il/i responsabile/i (qualora sia stato possibile individuarli);
- Ø Con la collaborazione dello psicologo della scuola, proporrà agli studenti attività durante le quali questi possano confrontarsi sull'accaduto;
- Ø La Referente del bullismo e cyberbullismo, con i docenti coordinatori di classe, si occuperà di tenere un Diario di bordo (vedi procedure) per monitorare la situazione all'interno dell'Istituto e poter pianificare specifiche azioni preventive;
- Ø Il Dirigente valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali.

Si precisa che i docenti, anche con l'ausilio tecnico dell'Animatore digitale, possono provvedere a conservare le prove della condotta incauta o scorretta rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto. Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente. E' importante che nessun adulto intraprenda azioni di contatto con il potenziale autore. Conservare la prova è utile per far conoscere l'accaduto, in base alla gravità, ai genitori degli alunni, al Dirigente scolastico, fino alle autorità competenti. Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e al Dirigente scolastico. In particolare, la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.

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.

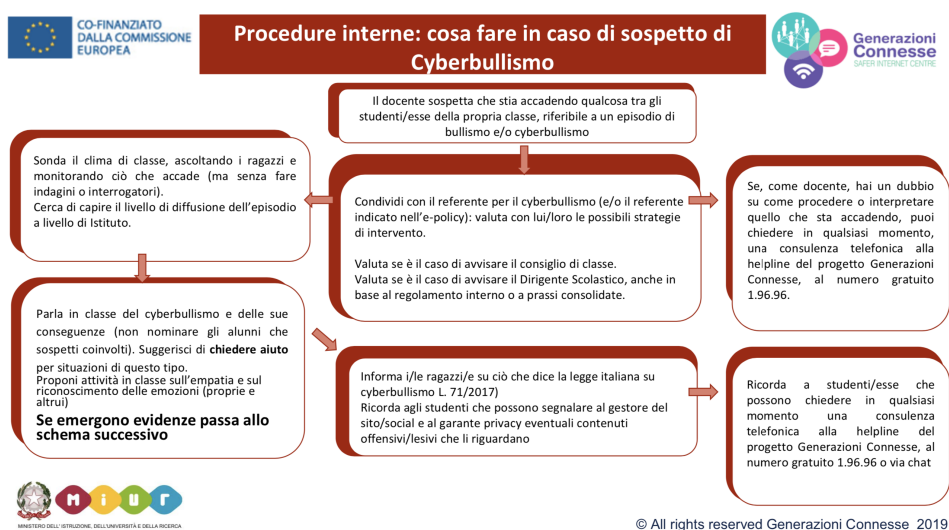
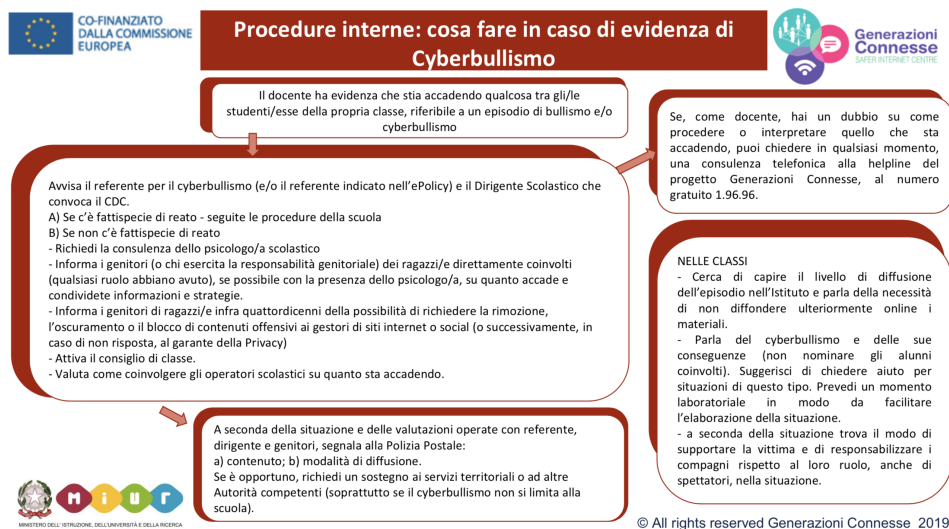
Per un'efficace gestione dei casi, nonché la segnalazione alla Dirigenza Scolastica ed eventualmente alle autorità competenti, il personale scolastico si attiene alle modalità illustrate nei protocolli suggeriti dal sito www.generazioniconnesse.it

Le autorità competenti conosciute sul Territorio sono principalmente il Commissariato Casilino e la Stazione dei Carabinieri di Tor Bella Monaca, che negli anni precedenti hanno svolto anche attività di prevenzione con le classi della scuola primaria e Secondaria di Primo Grado.

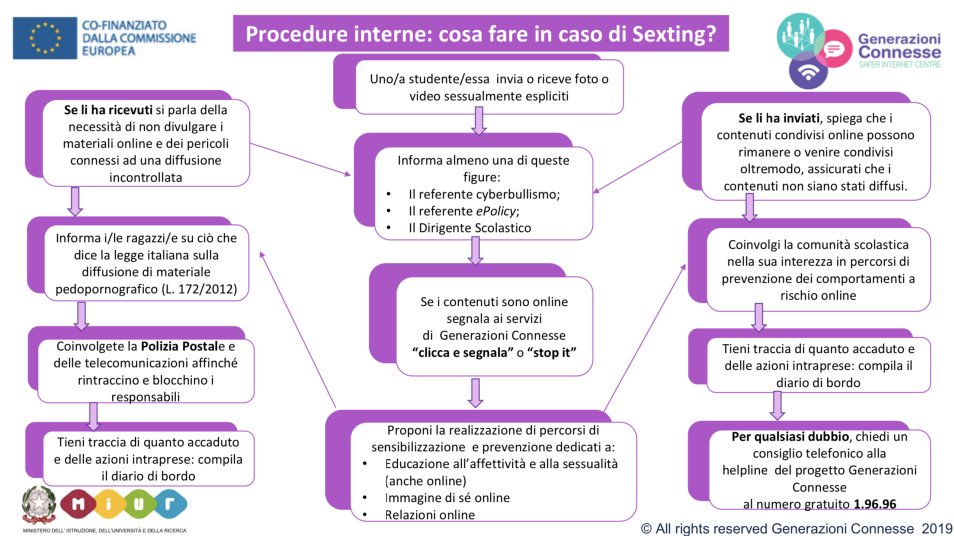
L'ASL RM2 ha attivi ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni ad esse correlate.

5.4. - Allegati con le procedure

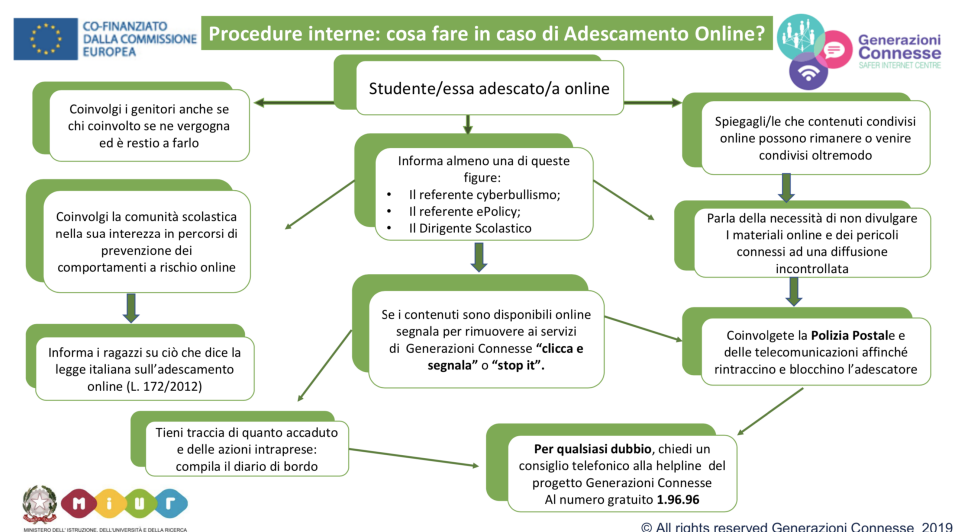
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



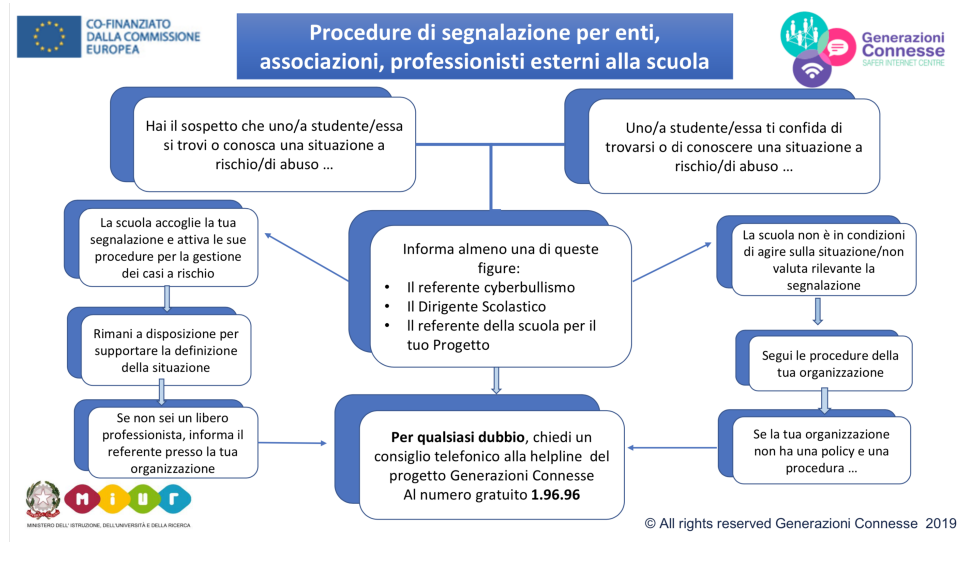
Procedure interne: cosa fare in caso di sexting?



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](#)

LINEE GUIDA PER ALUNNI:

- Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere e caratteri speciali;
- Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola;
- Non inviare a nessuno fotografie tue o di tuoi amici;
- Prima di inviare o pubblicare su un Blog la fotografia di qualcuno, chiedi sempre il permesso;
- Chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da Internet;
- Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola;
- Quando sei connesso alla rete, rispetta sempre gli altri: ciò che per te è un gioco può rivelarsi offensivo per qualcun altro;
- Non rispondere alle offese ed agli insulti;

- Blocca i Bulli: molti Blog e siti social network ti permettono di segnalare i cyberbulli;
- Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto;
- Se ricevi materiale offensivo (e-mail, sms, mms, video, foto, messaggi vocali) non diffonderlo: potresti essere accusato di cyberbullismo;
- Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE;
- Riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet;
- Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori;
- Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere;
- Non scaricare (download) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori;
- Non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso del tuo insegnante o dei tuoi genitori.

LINEE GUIDA PER INSEGNANTI:

- Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune;
- Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento dei dispositivi cancellare file di lavoro sparsi e al di fuori delle cartelle personali;
- Discutete con gli alunni della E-Safety Policy della scuola, di utilizzo consentito della rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet;
- Date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni saranno monitorate;

- Ricordate di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione su Internet del laboratorio (qualora sia stata attivata);
- Ricordate agli alunni che la violazione consapevole della E-Safety della scuola, di utilizzo consentito della rete, comporta sanzioni di diverso tipo;
- Adottate provvedimenti "disciplinari", proporzionati all'età e alla gravità del comportamento;
- Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni;
- Nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi;
- Chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indirizzo e-mail, ecc... ;
- Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro;
- In caso di abuso sessuale, rilevato anche attraverso i nuovi mezzi di comunicazione come internet o il cellulare, confrontatevi con i colleghi di classe e il Dirigente Scolastico, denunciate all'autorità giudiziaria o agli organi di Polizia.

CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA:

- Posizionate il computer in salone o in una stanza accessibile a tutta la famiglia;
- Evitate di lasciare le e-mail o file personali sui computer di uso comune;
- Concordate con vostro figlio le regole: quando si può usare internet e per quanto tempo;
- Inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l'accesso a siti pornografici;
- Aumentate il filtro del "parental control" attraverso la sezione sicurezza in internet

dal pannello di controllo;

- Attivate il firewall (protezione contro malware) e antivirus;
- Manifestate curiosità: chiedete a vostro figlio di mostrarvi come funziona internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante;
- Incoraggiate le attività on-line di alta qualità: ricercare informazioni scientifiche, ricercare nuovi amici nel mondo;
- Partecipate alle esperienze on-line: navigate insieme a vostro/a figlio/a, incontrate con lui/lei amici on-line, discutete gli eventuali problemi che si presentano;
- Spiegate a vostro figlio che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai fornita ai compagni o ad altre persone;
- Stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia);
- Discutete sul tema dello scaricare file e della possibilità di ricevere file con virus;
- Raccomandate di non scaricare file da siti sconosciuti;
- Incoraggiate vostro/a figlio/a a dirvi se vede immagini particolari o se riceve e-mail indesiderate;
- Discutete nei dettagli le conseguenze che potranno esserci se vostro/a figlio/a visita deliberatamente siti non adatti, ma non rimproveratelo/a se compie azioni involontarie;
- Spiegate a vostro/a figlio/a che le password, i codici pin, i numeri di carta di credito e i numeri di telefono e i dettagli degli indirizzi e-mail sono privati e non devono essere dati ad alcuno;
- Spiegate a vostro/a figlio/a che non tutti in Internet sono chi realmente dichiarano di essere;
- Il modo migliore per proteggere i vostri figli è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

PATTO BYOD (Bring Your Own Device - Porta il tuo dispositivo)

ALUNNI

Carissimo/a,

come studente/essa della classe ... della scuola primaria ".....", avrai la

possibilità di poter portare da casa a scuola il tuo device (dispositivo elettronico).

Sei un/a bambino/a bravo/a e responsabile e ti meriti questa opportunità che i tuoi genitori in accordo con i tuoi insegnanti hanno pensato di darti per poter svolgere alcuni lavori a scuola: imparare e divertirti.

Questa possibilità comprende alcune regole. Leggi bene il seguente contratto. Se non rispetterai queste regole i tuoi genitori ti toglieranno questa possibilità.

1. Il device appartiene ai tuoi genitori. Te lo stanno prestando e affidando per un breve periodo di tempo.
2. Appena torni a casa consegna prontamente il tuo device a uno dei tuoi genitori che lo spegnerà e/o metterà in carica se c'è bisogno.
3. Il device verrà a scuola con te solo quando te lo diranno i tuoi insegnanti.
4. Se il device si rompe o svanisce nel nulla, sei responsabile!

Quando sei in rete:

5. Cerca su internet contenuti di cui parleresti anche con i tuoi genitori. Se hai domande rispetto a qualsiasi cosa, chiedi a una persona adulta come mamma e papà e/o ai tuoi insegnanti.
6. Non scrivere qualcosa che non diresti di persona.

E ricorda sempre:

7. Quando sei in compagnia di altre persone puoi anche spegnerlo, non permettere al device di trasformarti in una persona maleducata.
8. Gioca a qualche gioco di parole o di logica che stimoli la tua mente, ogni tanto.
9. Tieni gli occhi aperti. Guarda cosa succede intorno a te. Guarda fuori dalla finestra. Ascolta il canto degli uccellini. Fai una passeggiata, fai lavorare la tua immaginazione anche senza device.
10. Se userai impropriamente il device ti verrà ritirato. Ci metteremo seduti e ne parleremo anche con i tuoi genitori. Ricominceremo da capo. Siamo qui per imparare cose nuove, giorno per giorno, insieme.

Speriamo che tu possa essere d'accordo su questi punti. Molte delle "lezioni" che fanno parte della lista non si applicano soltanto al device, ma anche alla vita. Fidati della tua testa e del tuo grande cuore, più che di ogni apparecchio.

Se rispetterai queste dieci regole potrai goderti questa nuova favolosa opportunità!

I tuoi insegnanti,

.....

Firma dell'alunno/a

Firma del/i genitore/i

DICHIARAZIONE DEI GENITORI

Il/La sottoscritto/a

genitore dell'alunno/a

frequentante la classe ... della scuola primaria ""

DICHIARA

- Di essere al corrente che, in ambito scolastico, i docenti introdurranno, a fianco degli strumenti e dei materiali didattici in uso a scuola, l'utilizzo di applicazioni, contenuti e servizi fruibili in locale e in Internet tramite dispositivi elettronici (device) propri;
- Di collaborare con i docenti nel responsabilizzare i ragazzi sulle modalità di accesso a internet e sulle regole a cui attenersi.

AUTORIZZA LA SCUOLA

- A creare un account personale al proprio figlio/a che permette l'accesso alle condivisioni on line e che include strumenti di comunicazioni (posta elettronica, video-chiamate). Lo strumento permette di ricevere ed inviare messaggi e comunicazioni solo con gli altri studenti e con i docenti della scuola.
- Al trattamento dei dati personali del proprio figlio (comprendendo anche fotografie e videoriprese) nella documentazione online delle attività didattiche svolte. L'accesso a queste pubblicazioni sarà consentito esclusivamente agli utenti del dominio della scuola (alunni, famiglie, docenti, dirigente scolastica, uffici).

Data

Firma del/i genitore/i

PATTO BYOD (Bring Your Own Device - Porta il tuo dispositivo)

GENITORI

Il / La sottoscritto/a

genitore dell'alunno/a.....

frequentante la classe ... della scuola primaria "....."

AUTORIZZA IL/LA PROPRIO/A FIGLIO/A

A portare a scuola il proprio dispositivo (specificare marca e modello accanto alla tipologia):

- TABLET
- SMARTPHONE
- VIDEO-GIOCO MULTIMEDIALE
- MICROFONO WIRELESS
- ALTRO

che sarà usato dallo studente a scuola, in modo individuale o in gruppo, per attività ed esperienze di apprendimento in rete, quali lo scambio e la produzione di materiali condivisi, con la guida e la supervisione dei docenti.

DICHIARA

che durante la permanenza a scuola del dispositivo il proprio figlio sarà responsabile della sua custodia e del suo uso corretto, secondo le regole e le disposizioni concordate con gli insegnanti.

Data

firma del/i genitore/i

Il nostro piano d'azioni

Organizzare e promuovere momenti di approfondimento che informino docenti, genitori e studenti/studentesse sulle procedure di rilevazione e segnalazione contenute nell'esafety policy.

