



I.C. - "LEONARDO SCIASCIA"-PALERMO
Prot. 0006780 del 25/05/2021
(Uscita)



Documento di ePolicy

PAIC870004

I.C. LEONARDO SCIASCIA-PA

VIA FRANCESCO DE GOBBIS13 - 90146 - PALERMO - PALERMO (PA)

Stefania Cocuzza

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.

In particolare **l'intento della scuola** è quello di:

- **promuovere l'uso consapevole** e critico da parte degli alunni delle tecnologie digitali e di internet
- **acquisire loro procedure e competenze "tecniche"** ma anche **corrette norme comportamentali**
- **prevenire** ovvero rilevare e **fronteggiare** le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali .

Gli utenti, soprattutto minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.

Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

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.

Dirigente scolastico

Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti:

- garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

Animatore digitale

Il ruolo dell'Animatore digitale, supportato dal Team dell'innovazione, include i seguenti compiti:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di Documento di e-policy prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

Referente del bullismo e cyberbullismo

Il referente del bullismo e cyberbullismo deve:

- coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo avvalendosi anche della collaborazione delle Forze di Polizia, Associazioni e centri di aggregazione giovanile del territorio;
- coinvolgere con progetti e percorsi formativi adatti studenti, docenti e genitori.

Direttore dei servizi generali e amministrativi

Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente

scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Docenti

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

Alunni

Il ruolo degli alunni include i seguenti compiti:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande, difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

Genitori

Il ruolo dei genitori degli alunni include i seguenti compiti:

- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;
- fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale.

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).

Le organizzazioni, associazioni e gli esperti esterni chiamati alla realizzazione di progetti e attività educative dovranno prendere visione dell'E-Policy dell'Istituto.

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/lle 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.

In particolare, si deve:

1. Condividere e comunicare la politica di e-safety agli alunni

Tutti gli alunni:

- saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale

saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione.

- L'istruzione degli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete;
- l'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet;
- sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.

2. Condividere e comunicare la politica di e-safety al personale

- La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;
- per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche essenziali;
- il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato;
- un'adeguata informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;
- il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;
- l'Animatore digitale metterà in evidenza on-line utili strumenti che il personale potrà usare con gli alunni in classe (questi strumenti varieranno a seconda dell'età e della capacità degli alunni) ;
- tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

3. Condividere e comunicare la politica di e-safety ai genitori

- L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree del sito web della scuola;
- sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;
- l'Animatore digitale fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa;
- l'Animatore digitale e i docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero.

1.5 - Gestione delle infrazioni alla ePolicy

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

1) Disciplina degli alunni

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

- un uso della rete per giudicare,
- infastidire o impedire a qualcuno di esprimersi o partecipare;
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime o troppo spinte;
- la comunicazione incauta e senza permesso con sconosciuti;
- il collegamento a siti web non indicati dai docenti.

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno. Infatti più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, 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.

2) Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni:

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni. Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

3) Disciplina dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico. Le situazioni familiari meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- una posizione del computer in una stanza o in un posto non visibile a tutti

quando è utilizzato dal proprio figlio;

- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;
- un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri

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.

La policy richiede l'integrazione con l'inserimento delle seguenti norme:

- Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
- Le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
- In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile

In caso di malfunzionamento non risolvibile dal responsabile di laboratorio, il suddetto contatterà la segreteria e poi il tecnico.

Disposizioni sull'uso dei software

1. I software installati sono ad esclusivo uso didattico.

2. In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale. Nei casi in cui lo fossero in base a precise norme contrattuali i docenti interessati, dopo aver concordato il prestito con il Responsabile di laboratorio, devono compilare l'apposito registro di consegna software custodito in laboratorio.

3. E' fatto divieto di usare software non conforme alle leggi sul copyright. E' cura dell'insegnante utente di verificarne la conformità. Gli insegnanti possono installare nuovo software sui PC del laboratorio della propria scuola, previa autorizzazione scritta del DS solo se il software installato rispetta le leggi sul copyright.

4. E' responsabilità degli insegnanti che chiedono al Responsabile di laboratorio di effettuare copie di cd/dvd per uso didattico, di assicurarsi che la copia non infranga le leggi sul copyright in vigore.

Accesso a internet

1. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;

2. Internet non può essere usato per scopi vietati dalla legislazione vigente;

3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;

4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza. Norme finali Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

ART. 49 - UTILIZZO DEL TELEFONO CELLULARE E DEI VARI DISPOSITIVI ELETTRONICI DURANTE LE ATTIVITÀ SCOLASTICHE

a) Salvo casi del tutto eccezionali, i telefoni cellulari non devono essere portati a scuola e non devono comunque essere utilizzati durante l'orario scolastico. Se - malgrado il divieto - gli studenti verranno sorpresi ad usare il cellulare, lo stesso verrà temporaneamente requisito dai docenti che registreranno l'episodio sul registro di classe e - in collaborazione con il personale ausiliario e/o con la segreteria - convocheranno per le vie brevi i genitori interessati ai quali verrà riconsegnato il cellulare requisito. Avuto inoltre riguardo per il fatto che i moderni cellulari possono essere utilizzati anche per scattare foto (o effettuare riprese filmate) e per trasferirle con un MMS, si informano i Sigg. genitori che eventi di questo tipo - se si concretizzano durante l'orario scolastico - si possono configurare anche come reati per i quali non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza.

b) L'Istituzione Scolastica non ha e comunque non si assume alcuna responsabilità né relativamente all'uso improprio o pericoloso che gli studenti dovessero fare del cellulare (es.: inviare/ricevere messaggi a/da soggetti ignoti agli stessi genitori), né relativamente a smarrimenti e/o 'sparizioni' di telefonini cellulari o di lettori mp3 o di hard/disk portatili o pen drive.

c) In ogni caso, i genitori tengano conto che le comunicazioni urgenti ed

improcrastinabili possono essere trasmesse ai loro figli durante l'orario scolastico rivolgendosi telefonicamente alle singole sedi scolastiche ovvero in Segreteria.

d) Il divieto ribadito per i telefoni/videotelefoni cellulari e per i lettori mp3 si estende ovviamente anche ad altri oggetti il cui uso a scuola può persino arrecare danni a terzi. A titolo meramente esemplificativo, si citano coltellini di vario genere, attrezzi multiuso con lame richiudibili, sigarette ed accendini ecc. Nelle situazioni in cui i docenti (ovvero i collaboratori scolastici) dovessero constatare che i ragazzi stanno usando o hanno con loro oggetti come quelli di cui si sta scorrendo, adotteranno la medesima procedura indicata all'art. 4 8, lettera g.

e) La scuola non pone alcun ostacolo all'utilizzo di cd/dvd rom o di hard - disk portatili come strumenti di lavoro e di studio. Ciò che a riguardo compete alle famiglie è il controllo periodico del contenuto di questi strumenti per evitare che qualche studente 'trasporti' a scuola immagini / testi / filmati per così dire 'sconvenienti', avendoli scaricati. Per impedire che le stesse postazioni dei laboratori scolastici possano essere furtivamente utilizzate per visitare siti volgari e pericolosi, la scuola si è da tempo dotata di un software di sicurezza che filtra gli accessi ad internet e protegge quindi i visitatori meno esperti. Oltre a questo sofisticato sistema di protezione che blocca l'accesso ai siti di cui si discorre, la scuola ovviamente mette in campo soprattutto la vigile attenzione educativa di ogni singolo docente.

f) Fermo restando il fatto che la scuola è un'istituzione educativa e che non è né prevista, né possibile, né tantomeno legittima la perquisizione quotidiana di tutti gli studenti all'inizio di ogni giorno di lezione, le responsabilità che dovessero derivare dal verificarsi di eventi riconducibili all'uso non corretto o non legittimo di uno qualsiasi degli oggetti di cui alla presente norma regolamentare sono tutte ascrivibili alle famiglie degli studenti eventualmente coinvolti. Le responsabilità appena menzionate sono condivise dal personale scolastico solo quando e solo se - avendo personalmente constatato o essendo venuto a conoscenza che qualche ragazzo/a ha con sé durante l'orario scolastico un oggetto potenzialmente pericoloso e/o il cui uso può compromettere la serenità del clima interno alla scuola non dovesse immediatamente intervenire nelle forme già indicate e comunque in modo tale da prevenire o reprimere sul nascere situazioni incompatibili con le più elementari regole della civile convivenza.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

Azioni da svolgere nei prossimi 3 anni:

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

regolamentare azioni e comportamenti.

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

Capitolo 2 - Formazione e curriculum

2.1. 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.

Il nostro Istituto si è dotato nell'anno scolastico 2018/2019 di un Curricolo di Cittadinanza e Costituzione, implementato quest'anno dal Curricolo di Educazione civica. All'interno di questo documento il nucleo fondante di Cittadinanza Digitale si basa sul DigComp 2.1 che permette di padroneggiare abilità e tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle nel rispetto degli altri e sapendone prevenire ed evitare i pericoli.

In particolare:

SCUOLA DELL' INFANZIA

Utilizzare le nuove tecnologie per giocare, con la supervisione dell’insegnante

- I computer
- Mouse

- Tastiera
- Eseguire giochi al computer o alla LIM
- Visionare immagini, opere artistiche, documentari Con la supervisione dell'insegnante,
- conoscere l'utilizzo del computer per attività .

SCUOLA PRIMARIA

- Usa le tecnologie in contesti comunicativi concreti per ricercare dati e informazioni e per interagire con soggetti diversi.
- Utilizzare le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio
- Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate
- Procedure per la produzione di testi.
- Procedure di utilizzo di reti informatiche per ottenere dati, fare ricerche, comunicare.
- Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini.
- Utilizzare materiali digitali per l'apprendimento
- Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago
- Utilizzare i mezzi informatici per redigere i testi delle ricerche, delle relazioni...;
- Utilizzare Internet e i motori di ricerca per ricercare informazioni, con la supervisione dell'insegnante

SCUOLA SECONDARIA DI PRIMO GRADO

- Utilizza con consapevolezza le tecnologie della comunicazione per ricercare le informazioni in modo critico.
- Usa con responsabilità le tecnologie per interagire con altre persone.
- Utilizzare le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio.
- Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate
- Le applicazioni tecnologiche quotidiane e le relative modalità di funzionamento
- Il sistema operativo e i più comuni software applicativi anche Open source
- Procedure per la produzione di testi, ipertesti, presentazioni.
- Procedure di utilizzo di reti informatiche per ottenere dati, fare ricerche, comunicare
- Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti in diverse situazioni.

- Utilizzare materiali digitali per l'apprendimento
 - Utilizzare il PC, periferiche e programmi applicativi
 - Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago
 - Utilizzare i mezzi informatici per redigere i testi delle ricerche, delle relazioni...
 - Utilizzare power point per effettuare semplici presentazioni
 - Utilizzare la posta elettronica per corrispondere tra pari, con istituzioni, per relazionarsi con altre scuole anche straniere;
 - Utilizzare Internet e i motori di ricerca per ricercare informazioni, con la supervisione dell'insegnante.
-

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.

Gli insegnanti devono raggiungere un buon livello di formazione in merito all'utilizzo e all'integrazione delle TIC nella didattica. L'Istituto, attraverso il Collegio dei Docenti, riconosce e favorisce la partecipazione del personale ad iniziative promosse sia dalla scuola, dalle Reti di scuole, dall'Amministrazione, sia da quelle scelte liberamente dai docenti, purché coerenti con il piano di formazione. Fondamentale porre attenzione all'uso del TIC nella didattica: un loro utilizzo strutturato e integrato rende gli apprendimenti motivanti, coinvolgenti ed inclusivi e permette al docente di guidare studenti e studentesse nella fruizione dei contenuti online, sempre più importante anche in ambito lavorativo (lavoro di gruppo anche a distanza, confronto fra pari in modalità asincrona)

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.

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

Verrà elaborato un cronoprogramma che consideri il triennio scolastico, in un'ottica di vera e propria programmazione, con azioni specifiche:

- Analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;
- Promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse".
- Monitorare le azioni svolte per mezzo di specifici momenti di valutazione;
- Organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc
- Sarà predisposta un'area specifica sul sito dell'Istituto con materiali formativi per gli insegnanti.

Nella sezione, saranno messi a disposizione materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet, prevedendo possibilità e modalità di condivisione fra gli insegnanti. Sempre sul sito istituzionale della scuola, è presente il link a Generazioni Connesse e, sarà predisposto materiale informativo con approfondimenti, spunti aggiornamenti e strumenti didattici utili da usare con gli studenti e le studentesse, per ciascun grado di scuola.

2.4. - Sensibilizzazione delle famiglie e

integrazioni al Patto di Corresponsabilità

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

Verrà Aggiornato il "Patto di corresponsabilità" con specifici riferimenti all'uso delle tecnologie digitali e all'ePolicy, per informare e rendere partecipi le famiglie sul percorso da intraprendere con il documento e il piano d'azione.

Il nostro piano d'azioni

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

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

digitali.

- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

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

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

Il nostro Istituto Scolastico in conformità al al Regolamento UE 2016/679 deve:

Valutare i rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili.

Le istituzioni scolastiche pubbliche e private possono trattare anche dati sensibili, come ad esempio dati relativi alle origini razziali per favorire l'integrazione degli/le alunni/e, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli/le alunni/e, come i dati vaccinali con le Asl.

Analizzare il processo sulla raccolta/gestione del consenso:

occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio, all'interno di modulistica o sul proprio sito web istituzionale.

Prestare attenzione alla formula utilizzata per chiedere il consenso:

deve essere comprensibile, semplice e chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, ma devono ad esempio adeguare tutta la modulistica al Regolamento UE 2016/679 e predisporre una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.

Adottare idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti:

- analisi del sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati proposte in messa in sicurezza della intranet scolastica sulle reti Wi-fi installate;
- utilizzo di black list per la navigazione (sistemi di filtraggio dei contenuti);
- uso di un firewall hardware (componente hardware che, utilizzando un certo insieme di regole predefinite, permette di filtrare ed eventualmente bloccare tutto il traffico da e verso una qualsiasi rete di computer, lasciando passare solo tutto ciò che rispetta determinate regole);
- istituire corsi di formazione destinati ai responsabili, agli incaricati ed eventualmente ai subincaricati del trattamento.

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.

In particolare però:

1. *L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;*

2. Internet non può essere usato per scopi vietati dalla legislazione vigente;
3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;
4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza. Norme finali Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

L'accesso a Internet è possibile e consentito per la didattica in tutti i plessi della primaria e della secondaria di primo grado attraverso reti WiFi.

Le impostazioni dei computer presenti nei laboratori e nelle aule sono definite e mantenute dal responsabile dei laboratori, il quale segnala alla segreteria eventuali malfunzionamenti e disservizi ed installa un filtro di protezione per la navigazione dei minori sui computer utilizzati dagli alunni per l'accesso ad Internet.

L'accesso a Internet, attraverso i dispositivi della scuola da parte degli studenti, avviene solo in presenza dell'insegnante, il quale è responsabile del comportamento degli alunni, delle macchine e del software che utilizzano. È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al personale di assistenza tecnica.

L'accesso ai portali istituzionali come SIDI, Istanze on-line, alla Segreteria Digitale, PON ecc. prevede l'uso di credenziali personali, mentre l'accesso a portali tematici si effettua per mezzo di password uniche condivise tra i referenti di progetti e/o azioni e la dirigenza. I docenti possono accedere alla propria sezione del registro elettronico con credenziali personali. I computer presenti nelle aule non richiedono una password di accesso per l'accensione.

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.

Il sito dell'Istituto Comprensivo è raggiungibile all'indirizzo <http://www.istitutosciascia.edu.it/>

La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione è a cura del Dirigente Scolastico e dei docenti referenti del sito web. Sul sito è possibile trovare il Regolamento d'Istituto, pubblicizzazione di eventi, avvisi ai genitori, documentazione di attività curricolari ed extracurricolari svolte; pulsanti attivi permettono l'accesso a link di interesse, tra cui il registro elettronico .

È possibile accedere all'area riservata del sito dove sono caricate le comunicazioni interne. L'accesso a tale area non è nominativo, ma è stata creata un'unica credenziale per tutti.

La scuola, in qualità di ente pubblico, pubblicherà sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

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.

Come da Regolamento d'Istituto agli studenti è fatto assoluto divieto di usare all'interno dell'Istituto scolastico, se non per scopi esclusivamente didattici

autorizzati dal docente, smartphone e/o ogni altro apparato multimediale
(walkman, mp3, ipod, ipad, notebook, fotocamera, videocamera, ecc...).

Il divieto non si applica soltanto all'orario delle lezioni, ma all'intera permanenza dell'alunno all'interno della struttura scolastica (intervalli, pausa mensa...). I predetti dispositivi devono essere tenuti spenti e opportunamente custoditi e depositati in borsoni, zaini, giacconi, giammai sul banco né tra le mani.

Come da Regolamento d'Istituto ai sensi della C.M. n.362 del 25/08/98, i docenti non possono utilizzare i telefoni cellulari durante l'orario di lavoro. E' consentito l'uso di dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.

Per il personale ATA della scuola: è vietato l'utilizzo di dispositivi elettronici durante l'orario di servizio.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

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

delle tecnologie digitali (cybersecurity)

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Le azioni di sensibilizzazione riguarderanno:

- accrescere la consapevolezza nel gruppo target di riferimento circa un determinato tema/bisogno/problema che potrebbe presentarsi in quel gruppo;
- incoraggiare il gruppo a modificare i propri comportamenti rendendoli più

funzionali;

- diffondere all'esterno del gruppo di riferimento e quindi tra l'opinione pubblica una certa consapevolezza rispetto all'argomento di interesse;
- facilitare il coinvolgimento di soggetti esterni in modo da mettere insieme diverse idee per lavorare ad un obiettivo comune.
- favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva (promuovere la conoscenza dell'ePolicy nella comunità scolastica).

In sintesi, è opportuno tenere in considerazione i seguenti aspetti:

spingere le persone a desiderare un cambiamento;

porre in evidenza la possibilità di generare un cambiamento;

individuare le azioni che consentono di produrre il cambiamento.

Se il problema della "sicurezza" è difficilmente riconducibile esclusivamente all'esistenza in sé di alcuni rischi, più o meno gravi e insidiosi, appare chiaro come le migliori strategie di intervento siano di carattere prevalentemente preventivo.

Prevenzione Universale

Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale. Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che "trattano" un gruppo con un problema specifico. Tuttavia, questi interventi possono produrre cambiamenti in grandi popolazioni (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale).

Prevenzione Selettiva

Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti. Prevenzione Indicata. Un programma di intervento sul caso specifico, è quindi pensato e strutturato per adattarsi agli/lle studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/lla ragazzo/a. La responsabilità dell'azione preventiva ed educativa chiama in campo diverse agenzie educative oltre alla scuola, come la famiglia, ma non

solo (istituzioni, associazioni, società civile, etc.), ciascuna con un proprio compito nei confronti di bambini e bambine e di adolescenti.

Tali agenzie sono chiamate a collaborare ad un progetto comune, nell'ambito di funzioni educative condivise. La necessità di questa collaborazione nasce, più o meno consapevolmente, dal riconoscimento sia da parte dei genitori che da parte degli insegnanti della rispettiva difficoltà a svolgere da soli la propria funzione formativa ed educativa.

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).

Le caratteristiche del fenomeno :

L'impatto: la diffusione di materiale tramite Internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online e continuare a diffondersi). Un contenuto offensivo e denigratorio online può, quindi, diventare virale e distruggere in alcuni casi la reputazione della vittima. Nelle situazioni più gravi, le vittime di cyberbullismo si trovano costrette a dover cambiare scuola o addirittura città, ma questo spesso non le aiuta. La Rete, si sa, è ovunque.

La convinzione dell'anonimato: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. Sentendosi protetti dall'anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. È importante tenere bene a mente, però, che quello dell'anonimato è un "falso mito della Rete". Ogni nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale. L'anonimato del cyberbullo, inoltre, è anche uno dei fattori che stanno alla base del forte stress percepito dalla vittima, la quale molte volte non può dare né un nome e né un volto al proprio aggressore;

L'assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio. La vittima può essere raggiungibile anche a casa e vive nella costante percezione di non avere vie di fuga. Spegnerne il cellulare o il computer non basta, così come cancellare tutti i propri profili social. Il solo pensiero che eventuali contenuti denigratori continuino a diffondersi online è doloroso e si accompagna ad un senso costante di rabbia e impotenza.

L'assenza di limiti temporali: può avvenire a ogni ora del giorno e della notte.

L'indebolimento dell'empatia: esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simile a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Tale sensazione è data dall'attivazione di una particolare area del cervello. Quando le interazioni avvengono prevalentemente online la funzione speciale di questi neuroni viene meno (mancando la presenza fondamentale dell'altro che è sostituito dal dispositivo). La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.

Il feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del

danno provocato. Per questo non è mai totalmente consapevole delle conseguenze delle proprie azioni. L'impossibilità di vedere con i propri occhi l'eventuale sofferenza e umiliazione provata dalla vittima fa sì che il tutto venga percepito come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi come non "reale", come un mondo ludico a sé stante.

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

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

cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

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

Come riconoscere casi di cyberbullismo?

Alcuni segnali generali che può manifestare la potenziale vittima di cyber bullismo

Appare nervoso quando riceve un messaggio o una notifica;

Sembra a disagio nell'andare a scuola o finge di essere malato (ha spesso mal di stomaco o mal di testa);

Cambia comportamento ed atteggiamento in modo repentino;

Mostra ritrosia nel dare informazioni su ciò che fa online;

Soprattutto dopo essere stato online, mostra rabbia o si sente depressa;

Inizia ad utilizzare sempre meno Pc e telefono (arrivando ad evitarli);

Perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;

Il suo rendimento scolastico peggiora.

La normativa in materia Il Parlamento italiano ha approvato il 18 maggio 2017 la Legge 71/2017, "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", una legge a tutela dei minori per la prevenzione e il

contrasto al cyberbullismo che prevede misure prevalentemente a carattere educativo/rieducativo. La legge pone al centro il ruolo dell'istituzione scolastica nella prevenzione e nella gestione del fenomeno e ogni Istituto scolastico dovrà provvedere ad individuare fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo. Questi aspetti vengono chiariti nel dettaglio dalle Linee di orientamento per la prevenzione e il contrasto del cyberbullismo. La L.71/17 introduce per la prima volta nell'ordinamento giuridico anche una definizione di cyberbullismo (come già riportato sopra). Nella consapevolezza che le azioni efficaci siano quelle che ricorrono agli strumenti educativi, rieducativi e di mediazione del conflitto, esistono tuttavia responsabilità da conoscere, la possibilità di commettere reati o danni civili e specifici dispositivi giuridici.

Sempre la Legge 71/2017 introduce un provvedimento di carattere amministrativo per gli autori di atti di cyberbullismo, la procedura di ammonimento da parte del Questore:

il minore autore può essere convocato dal Questore e ammonito se ritenuto responsabile delle azioni telematiche.

Più precisamente:

la procedura di ammonimento prevista in materia di stalking (art. 612-bis c.p.), in caso di condotte di ingiuria (art. 594 c.p.), diffamazione (art. 595 c.p.), minaccia (art. 612 c.p.) e trattamento illecito di dati personali (art. 167 del codice della privacy) commessi mediante internet da minori ultraquattordicenni nei confronti di altro minorenne, se non c'è stata querela o non è stata presentata denuncia, è stata estesa al cyberbullismo e può essere impartita da parte del questore (il questore convoca il minore, insieme ad almeno un genitore o a chi esercita la responsabilità genitoriale).

Gli effetti dell'ammonimento cessano al compimento della maggiore età. Chi compie atti di bullismo e cyberbullismo può anche essere responsabile di reati penali e danni civili. I ragazzi e le ragazze che fanno azioni di bullismo possono commettere reati. Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono: percosse (art. 581), lesione personale (art. 582), ingiuria (art. 594), diffamazione (art. 595), violenza privata (art. 610), minaccia (art. 612), danneggiamento (art. 635).

Cosa succede quando un minore commette un reato o procura un danno? Quali sono le responsabilità dei genitori e dei docenti/educatori?

Per il nostro ordinamento l'imputabilità penale (ossia la responsabilità personale per i reati commessi) scatta al quattordicesimo anno. La legge sancisce che "nessuno può essere punito per un fatto preveduto dalla legge come reato, se al momento in cui l'ha commesso, non era imputabile".

Cosa si intende per "imputabilità"? Vuol dire avere la cosiddetta "capacità d'intendere e volere"

Dunque, per poter avviare un procedimento penale nei confronti di un minore è necessario: che abbia almeno compiuto 14 anni; che, comunque, anche se maggiore di 14 anni, fosse cosciente e volente al momento del comportamento, cioè in grado di intendere e volere (tale non sarebbe, per esempio, un ragazzo con degli handicap psichici). L'atto di bullismo può violare sia la legge penale, sia quella civile, quindi può dar vita a due processi, l'uno penale e l'altro civile. Le responsabilità per atti di bullismo e cyberbullismo compiute dal minorenne possono ricadere anche su: i genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando). gli insegnanti e la scuola: perché nei periodi in cui il minore viene affidato all'Istituzione scolastica il docente è responsabile della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa. A pagare in primis sarà la scuola, che poi potrà rivalersi sul singolo insegnante. La responsabilità si estende anche a viaggi, gite scolastiche, manifestazioni sportive organizzate dalla scuola (culpa in vigilando). esiste poi una culpa in organizzando, che si ha quando la scuola non mette in atto le azioni previste per la prevenzione del fenomeno o per affrontarlo al meglio (così come previsto anche dalla normativa vigente).

Responsabilità dei genitori

Se il minore non ha compiuto i 14 anni, non risponde penalmente per l'evento, ma i genitori saranno tenuti al risarcimento del danno, per presunta "culpa in educando", così come previsto dal codice civile per i fatti commessi dal figlio. Non c'è responsabilità penale dei genitori, perché la responsabilità penale è personale. Se i genitori riescono a fornire la prova di aver fatto di tutto per impedire il fatto, possono essere esonerati dall'obbligo di risarcire il danno causato dal figlio. Ma questo tipo di prova è molto difficile da produrre, perché significa poter dare evidenza certa: di aver educato e istruito adeguatamente il figlio (valutazione che viene dal giudice commisurata alle circostanze, ovvero tra l'altro alle condizioni economiche della famiglia e all'ambiente sociale a cui appartiene), di aver vigilato attentamente e costantemente sulla sua condotta, di non aver in alcun modo potuto impedire il fatto, stante l'imprevedibilità e repentinità, in concreto, dell'azione dannosa.

Responsabilità degli insegnanti

Cosa succede nel caso di comportamenti penalmente rilevanti o di danni procurati ad esempio a scuola, durante una gita scolastica? In questi casi interviene l'art. 2048 del Codice Civile (responsabilità dei precettori) e l'art. 61 della L. 312/1980 n. 312 (responsabilità patrimoniale del personale direttivo, docente educativo e non docente). In base a queste norme, quindi, gli insegnanti sono responsabili dei danni causati a terzi "dal fatto illecito dei loro allievi... nel tempo in cui sono sotto la loro vigilanza". Se si tratta di una scuola pubblica, la responsabilità si estende alla pubblica amministrazione, che si surroga al suo personale nelle responsabilità civili derivanti da azioni giudiziarie promosse da terzi. Se si tratta di una scuola privata, sarà la proprietà

dell'Istituto a risponderne. Gli insegnanti potranno essere chiamati a rispondere personalmente solo in caso di azione di rivalsa per dolo o colpa grave, da parte dell'amministrazione. L'insegnante ha un dovere di vigilanza e di conseguenza viene addebitata, in caso di comportamento illecito del minore affidato, una colpa presunta, cioè una "culpa in vigilando", come inadempimento dell'obbligo di sorveglianza sugli allievi. colpa/responsabilità si può essere liberati dimostrando di non aver potuto impedire il fatto. Si tiene conto in questi casi dell'età e del grado di maturità dei ragazzi, della concreta situazione ambientale, etc. Inoltre, l'insegnante deve dimostrare di aver adottato in via preventiva le misure idonee ad evitare la situazione di pericolo. il Dirigente Scolastico qualora venga a conoscenza di atti di cyberbullismo deve informare tempestivamente i genitori dei minori coinvolti (art.5).

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.

1) Primo passo che intraprende il nostro Istituto nell'affrontare l'hate speech è fornire L'INFORMAZIONE del fenomeno agli alunni .

CHI COLPISCE L' *hate speech*:

- L'hate speech è fondato su elementi di discriminazione, colpisce nella dignità

le persone attaccate e mina il loro senso di sicurezza, in quanto individui già considerati socialmente vulnerabili e potenzialmente vittime di discriminazioni multiple. Quando l'attacco perpetrato attraverso l'hate speech è personale assume spesso la forma di trattamenti disumanizzanti o degradanti.

- **I discorsi d'odio si trasformano in etichette** con le quali è assegnata un'identità alle persone; **un marchio** che non viene apposto senza conseguenze: "L'attribuzione da parte di altri di identità inadatte e il divario tra queste e la percezione che ognuno ha di sé nuocciono al benessere psicologico e all'adattamento sociale dell'individuo [12]".

2) Il secondo passo che intraprende il nostro Istituto nell'affrontare l'hate speech è fornire la **CONOSCENZA** del fenomeno agli alunni :

Dichiarazione-universale-dei-diritti-umani.

Uguali in dignità e diritti: dalla Dichiarazione universale dei diritti dell'uomo [13]

- ART. 1: "Tutti gli esseri umani nascono liberi ed eguali in dignità e diritti. Essi sono dotati di ragione e di coscienza e devono agire gli uni verso gli altri in spirito di fratellanza".
- ART. 2: "Ad ogni individuo spettano tutti i diritti e tutte le libertà enunciate nella presente Dichiarazione, **senza distinzione alcuna, per ragioni di razza, di colore, di sesso, di lingua, di religione, di opinione politica o di altro genere, di origine nazionale o sociale, di ricchezza, di nascita o di altra condizione.** Nessuna distinzione sarà inoltre stabilita sulla base dello statuto politico, giuridico o internazionale del paese o del territorio cui una persona appartiene, sia indipendente, o sottoposto ad amministrazione fiduciaria o non autonomo, o soggetto a qualsiasi altra limitazione di sovranità".
- ART. 5 "Nessun individuo potrà essere sottoposto a tortura o a trattamento o a punizioni crudeli, inumani o degradanti".
- ART. 7 "Tutti sono eguali dinanzi alla legge e hanno diritto, senza alcuna discriminazione, ad una eguale tutela da parte della legge. Tutti hanno diritto ad una eguale tutela contro ogni discriminazione che violi la presente Dichiarazione come contro qualsiasi incitamento a tale

discriminazione”.

3) Il terzo passo che intraprende il nostro Istituto nell'affrontare l'hate speech è **CONTRASTARE** Il fenomeno agli alunni :

- **Tutela la tua identità**
- **Evita l'utilizzo di indirizzi email personali al momento della creazione di un account sui social network.**
- **Scegli password sicure e tra loro diverse per ogni account e indirizzo email.**
- **Crea un nuovo profilo Facebook per portare avanti l'attività di contrasto all'hate speech.**
- **Non rispondere a commenti e messaggi utilizzando account e indirizzi personali.**
- **Se gestisci un sito o una pagina web (un blog per esempio), assicurati che non vi siano informazioni tali da poter ricondurre alla tua identità.**
- **Quando ti colleghi, ricorri alla VPN - Virtual Private Network (online sono disponibili applicazioni e programmi scaricabili gratuitamente) per mascherare il tuo indirizzo IP.**
- **Quando pubblichi un contenuto, alcune applicazioni inseriscono anche la localizzazione: assicurati preventivamente di aver disattivato questa funzione.**
- **Non indicare tra le informazioni sui social network (o su altre piattaforme che prevedono questa possibilità) il tuo indirizzo privato, né quello della tua occupazione professionale.**

4) Il quarto passo che intraprende il nostro Istituto nell'affrontare l'hate speech è **VALUTARE L'IMPATTO** del fenomeno :

I punti da tenere a mente :

- **Il contenuto e il tono: da generalizzazioni negative (“Gli immigrati non lavorano”) a insulti moderati a espressioni estreme (“Troia, domani ti stupro”).**
- **L'intenzione dell'autore: “Eliminiamo i gay!” è sgradevole se scritto “per scherzo” in una email a un amico, ma è molto peggio se postato sulla pagina Facebook di una persona gay.**
- **I bersagli: se sono gruppi o individui vulnerabili, per come sono considerati nella società o nei media o per situazione personale. «Gli ebrei sono avidi e malfattori» è più pericoloso che «i politici sono avidi e**

malfattori».

- **Il contesto: le circostanze storiche e culturali, il mezzo impiegato, il pubblico raggiunto, l'autorità dell'autore, le tensioni verso il gruppo bersaglio.** "Gli immigrati rovinano il paese" è male sul blog di un 16enne, ma è molto peggio come tweet di un ministro.
- **L'impatto reale o potenziale su individui, gruppi, società; la percezione di chi ne è colpito spesso conta più delle impressioni dell'autore o di terzi.**

5) Il quinto passo che intraprende il nostro Istituto nell'affrontare l'hate speech è SAPER INTERAGIRE:

Quando rispondiamo a un post o a un tweet, oppure a un commento, dobbiamo ricordare che dietro a quel testo o a quella immagine c'è una persona. Come relazionarci con lei/lui?

- **Non essere aggressivo ma assertivo:** affermare le proprie tesi in modo chiaro e diretto ma rispettoso, esigendo a nostra volta rispetto.
- **Consideriamo l'interlocutore** non come incarnazione di una categoria ma **come persona**, ed esigiamo che faccia lo stesso verso di noi e coloro di cui si parla. Possiamo dargli del lei e chiamarlo per nome: "Buongiorno Mario, può spiegarmi cosa intende?". Chiediamogli se intendeva davvero quanto affermava, se lo direbbe nel mondo reale, ripetendoglielo con parole diverse.
- **Non usare termini che creino tifoserie** contrapposte quali "razzista", "ignorante" o "buonista".
- Se ci si confronta su un testo, invitiamo a leggerlo per intero per essere certi che lo conosca.
- **Invitiamo a restare in tema** (evitando il benaltrismo) e a non generalizzare: il crimine di un singolo non colpevolizza l'intero gruppo.

- **Chiediamo le fonti di un'affermazione**, e chiarimenti se è confusa. Mostriamo comprensione dello stato d'animo che ha portato a certe affermazioni.
- Usiamo l'ironia solo se sappiamo padroneggiarla, per esempio per sdrammatizzare e non per aggredire. Interagire con l'altro

6) Il sesto passo che intraprende il nostro Istituto nell'affrontare l'hate speech è SEGNALARE il fenomeno :

quando vi imbattete in un contenuto che ritenete essere hate speech, su Facebook o su Twitter, potete segnalarlo al social network chiedendone la rimozione. È importante, in entrambi i casi, leggere gli standard della comunità, per capire quali sono quei post e quei tweet che violano le regole dei rispettivi social network ed evitare così di segnalare contenuti che non hanno alcuna possibilità di essere rimossi.

Le conseguenze della segnalazione:

- **"Contenuto offensivo"; un post in un gruppo si può anche segnalare all'amministratore; in tal caso Facebook non riceverà la segnalazione; l'amministratore saprà chi lo ha segnalato, e potrà rimuovere il post o bloccare l'autore; chi non ha un account Facebook, o non può vedere il contenuto offensivo, può chiedere a un amico di segnalarlo, o compilare un memo** Il social valuta se i contenuti segnalati violino le proprie norme: gli Standard della comunità di Facebook e le Regole di Twitter (su Centro assistenza/Regole e norme di Twitter).
- **Twitter valuta le segnalazioni e prende eventuali provvedimenti a seconda della gravità e dei precedenti dell'utente.**
- **Per violazioni lievi e occasionali può oscurare il tweet e avvertire l'autore perché lo rimuova.**
- **Per violazioni gravi o ripetute può limitare temporaneamente l'attività dell'account (permettendone solo la lettura), sospenderlo, verificarne la proprietà (per evitare che il titolare ne usi altri), o chiuderlo definitivamente.**
- **Anche Facebook adotta provvedimenti graduati, dalla rimozione di singoli contenuti alla sospensione temporanea o permanente dell'account. Spesso i social hanno scelto di non rimuovere contenuti d'odio anche evidenti, ma col crescere delle pressioni sociali e normative la tolleranza per l'hate speech sta diminuendo.**
- **Su Facebook puoi conoscere l'esito delle tue segnalazioni controllando il riepilogo: nella barra di ricerca inserisci "Messaggi assistenza" e clicca sul risultato. Su Twitter, purtroppo, non esiste un servizio analogo**

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?

L' Istituto si impegna a promuovere conferenze di varia natura rivolte a genitori, insegnanti e studenti, formazione specifica rivolta ai docenti, attivazione di supporto psicologico e azioni di sensibilizzazione. Sono stati inoltre attivati diversi progetti che coinvolgono gli alunni durante le ore pomeridiane a scuola in modo che si allontanino dall'utilizzo sfrenato di internet in maniera non costruttiva.

4.5 - Sexting

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

Il sexting riguarda infatti, in senso lato, lo scambio di messaggi non solo di testo, ma anche foto e perfino video che potremmo definire "osé" o "spinti".

La sua diffusione è certamente legata alla facilità di accesso alle principali applicazioni di messaggistica istantanea, ai social network e all'utilizzo dello smartphone, diventato per i più giovani, dalla generazione Z - i nati tra il 2000 e il 2013 - alla generazione Alpha - i nati dopo il 2010, un'appendice imprescindibile.

Alla base però vi è un immaturo e narcisistico bisogno di apparire per essere: "postato"

dunque sono.

La vita virtuale, dove non viene governata, tende a prendere il sopravvento e a creare una correlazione necessaria con quei like e quei cuoricini che attestano la popolarità di un ragazzo o di una ragazza tra i suoi pari. Così si misura anche la possibilità di essere accettati e apprezzati dal gruppo per alimentare la propria autostima.

La consuetudine di scattare selfie ha spinto i ragazzi ad andare oltre, a condividere immagini senza abiti o a sfondo sessuale con il proprio ragazzo o la propria ragazza, ma anche nelle chat di gruppo.

Quello che emerge in modo evidente è che il luogo per eccellenza dove avviene la condivisione di materiale con chiaro riferimento sessuale sia WhatsApp, con una percentuale del 91%. A seguire, ma a grande distanza, anche Instagram (42,5%) e Snapchat (22%). Molto lontano, secondo la percezione dei ragazzi intervistati ma anche dei partecipanti ai gruppi di discussione, troviamo Kik (4%) ultimamente noto alle cronache proprio per la sua peculiare predilezione nell'essere il "social del sexting".

Al primo posto tra le motivazioni, per maschi e femmine, si trova "per essere popolare", seguito da "per divertirsi" nei maschi e "per ricevere ricompense materiali (ricariche, regali, vestiti, soldi...) nelle femmine, che scende al terzo posto nella graduatoria dei maschi.

Sexting e scuola

La scuola è il contesto educativo in cui il ragazzo trascorre la maggior parte del suo tempo; nell'arco dei nove mesi cresce relazionandosi con i propri pari in classe e con le ragazze e i ragazzi delle classi accanto, diversi per età.

A livello preventivo, è importante che vengano attivati all'interno dell'istituto scolastico percorsi di formazione rivolti ai ragazzi, ai docenti e ai genitori per approfondire i rischi e le conseguenze di episodi di sexting.

È importante offrire spunti per avviare il dialogo in classe con gli studenti, partendo da storie accadute o da fatti di cronaca da commentare per riflettere sui punti salienti:

- Consapevolezza del proprio valore e della propria immagine
- L'importanza di agire quanto prima, parlandone con una figura adulta
- Rispetto e responsabilità

- **Forme sanzionatorie e di tutela**

I docenti, come i genitori, devono essere aggiornati costantemente sui linguaggi in codice e gli acronimi utilizzati dai ragazzi, spesso difficili da individuare, perché non vogliono farsi capire dagli adulti quando parlano di sesso.

Come intervenire a scuola

Ogni istituto scolastico, in virtù dell'autonomia di cui gode nell'indicare le proprie scelte educative e organizzative è tenuto a redigere

- il "regolamento di Istituto"
- il "patto di corresponsabilità tra scuola e famiglia",

che potranno essere rivisti nell'ottica di prevenire e contrastare episodi di sexting.

Anche il nostro Istituto ha messo in atto delle sanzioni per contrastare il fenomeno:

- Nei casi più gravi (sexting, cyberstalking, cyber bashing...) l'Istituto scolastico sanzionerà con l'allontanamento fino a quindici giorni con o senza obbligo di frequenza.
- L'istituto valuterà la partecipazione dello studente ad attività utili alla maggiore consapevolezza del gesto compiuto"
- Obbligo di rimozione del materiale dal proprio profilo.
- Sarà coinvolta la polizia postale o altra forza dell'ordine per ipotesi di colpa in educando coinvolgendo DS / Consiglio di classe / Consiglio di Istituto

In generale l'indicazione è che:

- in caso in cui un insegnante venga a conoscenza di un episodio di sexting che coinvolga gli studenti del proprio istituto,
- notifichi il fatto al referente del cyberbullismo e al dirigente scolastico procedendo poi alla segnalazione all'autorità giudiziaria.

La notifica alle famiglie dovrà chiaramente tenere in considerazione la tutela del minore coinvolto. L'insegnante in questo caso si assume una grande responsabilità e riveste un delicato compito in quanto è la figura che all'interno della scuola si trova più vicino al ragazzo, ha la possibilità di osservarlo quotidianamente e di notare variazioni nel comportamento e soprattutto conosce il contesto di provenienza.

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.

E' necessario ricordare che si tratta di situazioni ad altissimo potenziale di rischio.

I percorsi di adescamento, anche detto grooming, hanno un'escalation molto variabile in relazione all'età della vittima, alla capacità dialettica del pedofilo, alla disponibilità di mezzi informatici: talvolta 20 occorrono mesi perché la vittima accetti contatti e avances, a volte in mezz'ora si definisce un appuntamento reale.

E' inoltre importante riportare che la casistica che arriva all'attenzione del CNCPO dimostra che sempre più spesso i tentativi di adescamento sono aggravati, nel giro di qualche battuta, da dinamiche di molestia e minaccia: l'abusante minaccia di divulgare immagini e conversazioni intime sul web se il minore non accondiscende alle richieste sessuali dell'adulto.

I livelli di sofferenza e paura possono quindi arrivare velocemente a intensità estreme.

L'adescamento è un reato procedibile d'ufficio, cioè un reato che non necessita di una denuncia formale della vittima perché si possa avviare un'attività di polizia giudiziaria tesa ad identificare il presunto abusante (indagine).

In qualità di pubblico ufficiale :

l'insegnante che venga a conoscenza in modo sufficientemente circostanziato di contatti sessualizzati tra una studentessa/studente e un adulto in rete è tenuto a riferire in forma scritta al Dirigente Scolastico quanto ha appreso.

Il Dirigente Scolastico dovrà formalizzare con apposita denuncia all'Autorità

Giudiziaria (Procura) o alle forze dell'ordine quanto riferito dall'insegnante.

Sarà cura del **Dirigente Scolastico, congiuntamente all'insegnante** che ha avuto notizia dell'adescamento, informare tempestivamente i genitori della vittima della situazione di rischio, cercando di non indurre nei genitori stessi sentimenti di colpevolizzazione o di giudizio che non giovano alla protezione della vittima stessa.

Occorre ricordare inoltre che, secondo quanto previsto dall'art.351 c.p.p modificato dalla Legge n. 172/2012, l'ascolto per esigenze giudiziarie di qualsiasi vittima minorenne di reati di adescamento, violenza sessuale, pedopornografia dovrà essere effettuato alla presenza di un esperto in psicologia o psichiatri infantile.

La presenza dell'"esperto" garantirà che siano adottate tutte le cautele necessarie a rendere la raccolta delle informazioni utili alle indagini più rapida possibile, adattata alle capacità linguistiche in via di sviluppo, nel massimo rispetto delle fragilità specifiche ed evolutive di ogni singola vittima.

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](#).

Le azioni da intraprendere in relazione a questa problematica sono legate a percorsi di Educazione Civica, Affettiva e Sessuale; sensibilizzazione all'uso corretto e consapevole di Internet e del cellulare.

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

Il nostro piano d'azioni

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

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle

studenti/studentesse, con il coinvolgimento di esperti.

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

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

☐ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

☐ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

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

☐ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

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

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

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.

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).

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; raccolgono 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.

Contatti a Palermo

Tribunale per i Minorenni : via Principe di Palagonia n. 135 Palermo tel.091 68668211 email: tribmin.palermo@giustizia.it

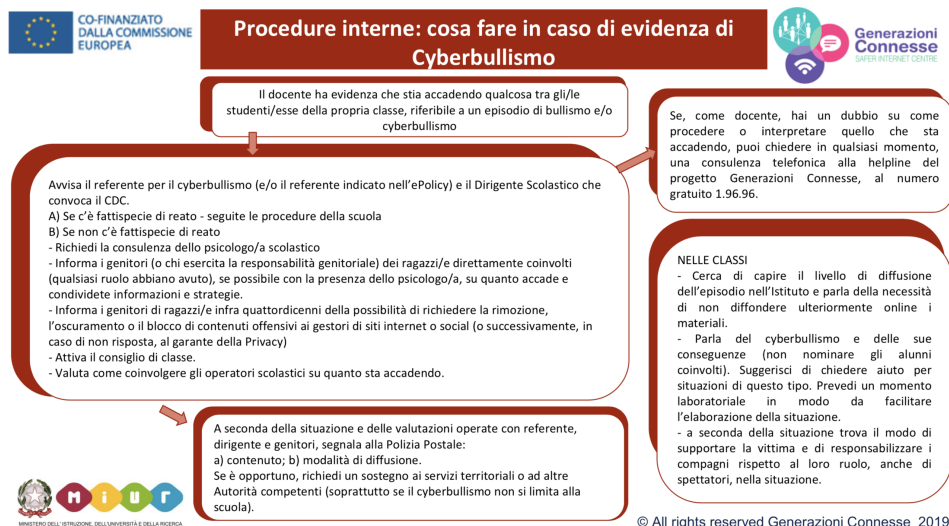
Comitato Regionale Unicef: via Isidoro La Lumia , 19/C Palermo tel. 091 681065 email: m.ferrara@unicef.it

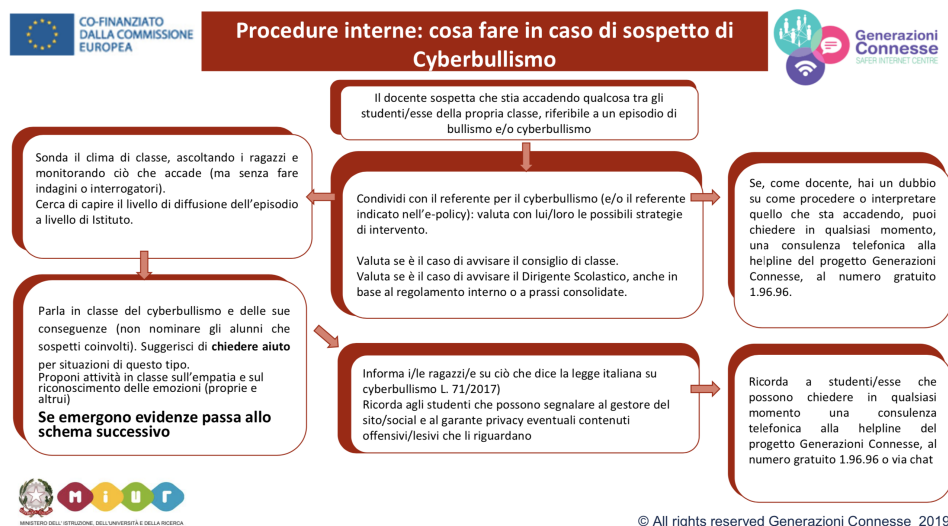
Co.Re.Com. : via Generale Magliocco, 46 Palermo email:corecom@regione.sicilia.it

Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico: Giuseppe Vecchio via Trinacria n. 44/36 tel. 0917074126

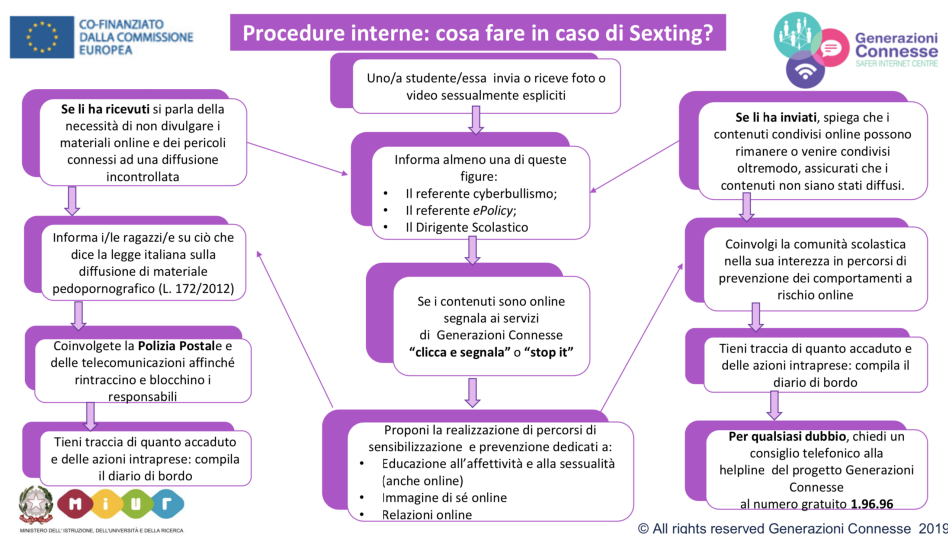
5.4. - Allegati con le procedure

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

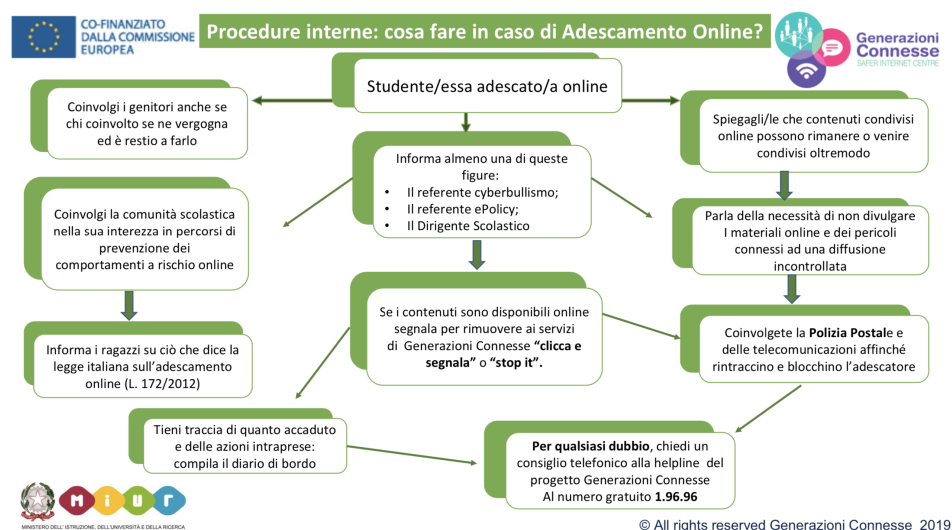




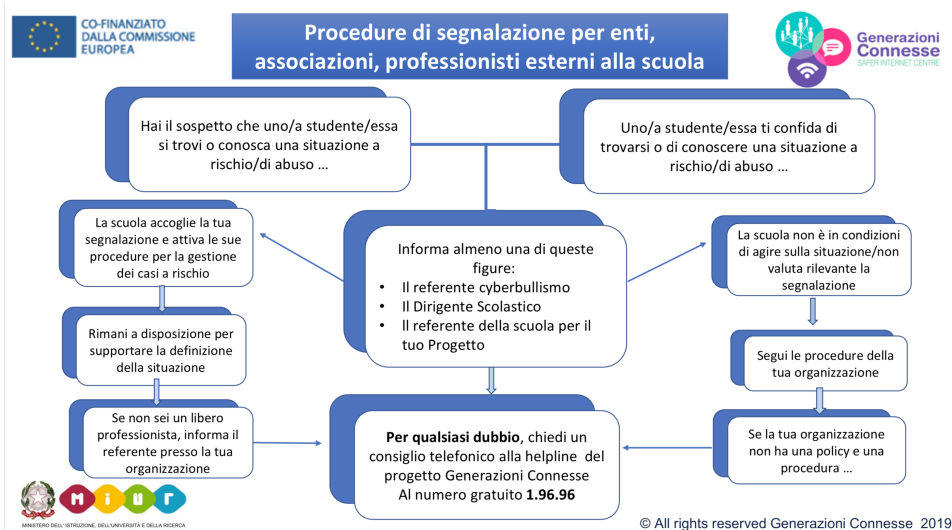
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

La Scuola si impegna ad organizzare le seguenti attività di prevenzione al fenomeno: organizzazione di Corsi di formazione per docenti, genitori, operatori del settore socioeducativo; partecipazione da parte di docenti, studenti e genitori a convegni e seminari sul tema del bullismo e del cyberbullismo; interventi di consulenza e supporto - su richiesta da parte della scuola - relativamente a casi di cyberbullismo.

