Documento di ePolicy

MIIS09200P

E.ALESSANDRINI - MAINARDI

VIALE ZARA23/C - 20010 - VITTUONE - MILANO (MI)

CARMELA PISANI

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 curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

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.

Con l'introduzione dell'ePolicy nella scuola, il nostro istituto ha l'obiettivo di promuovere un uso consapevole delle nuove tecnologie tra i giovani studenti oltre che sviluppare le competenze digitali e prevenire i rischi della "vita online". L'ePolicy è uno strumento fondamentale per affrontare le sfide del mondo digitale.

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.

Per quanto riguarda la corresponsabilità educativa si ricorda che esistono tre tipi di "reati": culpa in vigilando, imputabile al docente, culpa in organizzando imputabile al DS, e culpa in educando imputabile ai genitori. Quindi tutti i soggetti sono tenuti ad essere informati sui contenuti del documento, a cui verrà data la massima diffusione.

Ruolo	**Responsabilità**
DIRIGENTE SCOLASTICO	- è il responsabile della sicurezza dei dati - è il garante dell'applicazione della e-policy - individua referente per il bullismo e cyber bullismo - si impegna a garantire a tutti i docenti ed alunni, soprattutto quelli in entrata, la formazione per l'uso responsabile e corretto delle Tecnologie dell'Informazione e della comunicazione (alcune ore di lezione all'anno sulla websecurity nelle TIC), oltre che nell'uso personale, anche nella didattica, in collaborazione con il team digitale - si impegna a dotare la scuola di un sistema in grado di consentire il controllo della sicurezza in rete - si impegna a seguire le procedure relative agli eventi dannosi eventualmente occorsi agli alunni nell'utilizzo delle TIC a scuola.

ANIMATORE DIGITALE	- promuove la formazione interna in ambito tecnologico-digitale oltre che a fungere da referente per ogni informazione riguardo i rischi della rete, le relative misure di prevenzione nonché la gestione operativa delle eventuali problematiche - rileva e/o raccoglie le criticità proponendo soluzioni adeguate e sostenibili - si interessa dell'aggiornamento delle politiche di istituto sulla sicurezza della rete della scuola, e della proposta di novità ed aggiornamento metodologico e tecnologico implementabile nella rete di istituto ad uso di tutto il personale scolastico; - si impegna a gestire e controllare l'accesso alla rete ed ai servizi di istituto (posta elettronica,Gsuite,ecc.) da parte degli utenti mediante credenziali personalizzate, firewall, antivirus, ecc. - individua in collaborazione con le figure di sistema e il referente del bullismo e cyberbullismo progetti ed attività aventi ad oggetto la sicurezza in rete in cui coinvolgere la comunità scolastica.
REFERENTE CYBERBULLISMO	- promuove attività, eventi funzionali alla prevenzione delle problematiche inerenti al cyber bullismo e al tema della sicurezza in Rete.
DSGA	- assicura, nei limiti delle risorse finanziarie, la manutenzione delle strutture informatiche ai fini del suo funzionamento, della sua sicurezza e tutela da un uso improprio, e da attacchi esterni - garantisce la comunicazione all'interno dell'istituto, (sportello, circolari, sito web, ecc.), e tra le reti di scuole e fra la scuola e le famiglie degli alunni per la diffusione di informazioni nell'ambito dell'utilizzo delle tecnologie digitali e della rete.

DOCENTI	Hanno il compito di: - informarsi ed aggiornarsi su tema della sicurezza in rete uniformandosi alle politiche di sicurezza adottate dalla scuola di cui rispettano il regolamento - integrare nel curriculum di studio e nelle attività didattiche ed educative delle classi le modalità di utilizzo corretto e sicuro delle TIC e di Internet - assicurarsi 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. 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 - supportare gli alunni nel corretto utilizzo delle tecnologie digitali per finalità didattico-educative (controllo nel rispetto delle leggi, del regolamento interno, del plagio, del diritto d'autore, ecc), guidandoli nella scelta delle fonti di informazione - garantire che le comunicazioni con i mezzi informatici avvengano nel rispetto dei ruoli e dei rispettivi codici comportamentali, mediante canali ufficiali e verificabili (posta elettronica col dominio dell'istituto, G-suite, ecc.) - rispettare l'obbligo di riservatezza dei dati personali trattati e non, in conformità alla normativa vigente - interagire con i genitori, coordinando con gli stessi l'intervento educativo, nei casi di disagio, manifestato dall'alunno, collegato all'utilizzo delle tecnologie digitali - segnalare all'Animatore digitale eventuali criticità nei sistemi informativi soprattutto in materia di prevenzione e gestione dei rischi nell'uso delle TIC - seguire le procedure interne di segnalazione di eventuali abusi subiti dagli alunni e connessi all'uso delle tecnologie digitali
ALUNNI	Devono imparare a: - utilizzare responsabilmente le tecnologie digitali uniformandosi alle indicazioni dei docenti nonché rispettando le norme codificate nei regolamenti di istituto - rispettare le buone pratiche di sicurezza in rete - saper distinguere, con l'aiuto dei docenti, le fonti di informazione attendibili in rete per utilizzarle in modo appropriato senza violazione dei diritti d'autore altrui; - comunicare in rete in modo appropriato rispettando le posizioni altrui - segnalare ai genitori e/o ai docenti situazioni di difficoltà o di bisogno di aiuto nell'utilizzo delle tecnologie digitali - segnalare a docenti e/o genitori casi di abuso nell'utilizzo dei social a scuola
GENITORI	Hanno il compito di: - sostenere i docenti nell'azione educativa diretta al corretto utilizzo delle tecnologie digitali - educare, vigilando sui propri figli, al corretto utilizzo delle tecnologie digitali in ambiente domestico fissando regole comportamentali e di utilizzo - collaborare con i docenti nell'adozione di linee di intervento coerenti per contrastare l'uso non responsabile, scorretto o pericoloso delle tecnologie digita
PERSONALE A.T.A.	- è tenuto a conoscere e mettere in pratica i regolamenti redatti dall'Istituto - a segnalare tempestivamente eventuali violazioni. - a partecipare alle attività di formazione proposte in istituto

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).

Ogni volta che ci si avvale di soggetti esterni per ampliare l’offerta formativa dell’Istituto è bene che siano informati sui contenuti essenziali del documento di e-policy per quanto riguarda l’insieme di regole e di norme di comportamento da seguire e le procedure di segnalazione nel caso si rilevino infrazioni. Essi 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). A chi, in qualità di soggetto esterno, farà attività all’interno dell’istituto verrà data una sintesi del documento di e-policy.

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.

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.

Le infrazioni più comuni in cui possono incorrere gli studenti sono:
- 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.

I possibili provvedimenti “disciplinari”, proporzionati alla gravità del comportamento vengono riportati nel Regolamento di Disciplina. In particolare se si concretizzano durante l’orario scolastico episodi che si possono configurare come reati non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza.

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. Anche alcune condizioni e condotte dei genitori possono favorire o meno l’uso corretto e responsabile delle TIC da parte degli alunni a scuola, in particolare una piena autonomia concessa al proprio figlio nella navigazione sul web e nell’utilizzo del cellulare o dello smartphone. Da qui l’importanza di coinvolgere i genitori 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.

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

1.7 - Monitoraggio dell’implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone. Il monitoraggio e la revisione del documento ePolicy viene affidato al docente referente coadiuvato dal gruppo di lavoro e, ove possibile, con la partecipazione dell'animatore digitale.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

Azioni da svolgere nei prossimi 3 anni:

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

Capitolo 2 - Formazione e curricolo

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 curricolo digitale.

COMPETENZE (**DigComp 2.1**)

Area di competenze 1: Alfabetizzazione su informazioni e dati

1.1 Navigare, ricercare e fltrare dati, informazioni e contenuti digitali 1.2 Valutare dati, informazioni e contenuti digitali 1.3 Gestire dati, informazioni e contenuti digitali

Area di competenze 2: Comunicazione e collaborazione

2.1 Interagire attraverso le tecnologie digitali 2.2 Condividere informazioni attraverso le tecnologie digitali 2.3 Esercitare la cittadinanza attraverso le tecnologie digitali 2.4 Collaborare attraverso le tecnologie digitali 2.5 Netiquette 2.6 Gestire l'identità digitale

Area di competenze 3: Creazione di contenuti digitali

3.1 Sviluppare contenuti digitali 3.2 Integrare e rielaborare contenuti digitali 3.3 Copyright e licenze 3.4 Programmazione

Area di competenze 4: Sicurezza

4.1 Proteggere i dispositivi 4.2 Proteggere i dati personali e la privacy 4.3 Proteggere la salute e il benessere 4.4 Proteggere l'ambiente

Area di competenze 5: Risolvere problemi

5.1 Risolvere problemi tecnici 5.2 Individuare fabbisogni e risposte tecnologiche 5.3 Utilizzare in modo creativo le tecnologie digitali 5.4 Individuare divari di competenze digitali

Sono state individuate per il nostro Istituto le seguente aree tematiche:

1° anno: Saper conoscere e saper informarsi.

2° anno: Diritti del cittadino e abusi del web.

3° anno: Big data.

4° anno: Dipendenze e rete.

5° anno: Difesa e protezione dei dati.

Ogni nucleo tematico sarà sviluppato in termini di contenuti, abilità e competenze e acquisizione di specifici atteggiamenti in relazione ai discenti.

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

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

apprendimenti.

La competenza digitale, oggi, è imprescindibile per i docenti così come per studenti e studentesse e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento. Gli insegnanti, dunque, dovrebbero essere pronti a cogliere tale sfida anche grazie alla possibilità di formazione permanente offerta loro in primis dall'Istituto scolastico, in modo da rispondere ai diversi bisogni formativi della classe. L'obiettivo dell'IIS Alessandrini Mainardi è quello di programmare e realizzare corsi di formazione che coinvolgano i docenti sull'utilizzo delle TIC nella didattica.

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.

Il nostro istituto provvederà a realizzare specifici momenti di formazione per gli insegnanti che mettano al centro i temi in oggetto, considerando anche percorsi di autoaggiornamento personali o collettivi. Si utilizzerà un cronoprogramma che andrà a considerare il triennio scolastico, in un'ottica di programmazione e 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 e delle tecnologie digitali.

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.

La scuola come prima azione aggiornerà il "Patto di corresponsabilità" con specifici riferimenti all'uso delle tecnologie digitali e all'ePolicy. Si procederà ad informare i genitori sulle condotte da adottare a scuola e da mettere in pratica con i propri figli. A tale scopo si provvederà a:

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

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024)

- 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.

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

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

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

Il nostro istituto si è adeguato alla suindicata normativa adempiendo a quanto in essa prescritto. E' stata attivata una specifica sezione Privacy sul sito web dell'istituto dove sono state pubblicate tutte le informative e i relativi moduli per l'acquisizione dei consensi, i dati del Data Protection Officer (DPO), la politica sulla protezione dei dati personali, il vademecum "La scuola a prova di Privacy". Infine, si è provveduto a dotarsi del registro dei trattamenti nonché degli accorgimenti tecnici e strutturali idonei al fine di tutelare il diritto alla riservatezza dei componenti la comunità scolastica.

3.2 - Accesso ad Internet

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

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

reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

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

Il regolamento d'istituto prevede una parte dedicata all'uso di Internet in cui gli studenti dovranno impegnarsi a:

- utilizzare la rete nel modo corretto
- rispettare le consegne dei docenti
- non scaricare materiali e software senza autorizzazione
- non utilizzare unità removibili personali senza autorizzazione
- tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo
- durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste
- segnalare immediatamente materiali inadeguati ai propri insegnanti.

I docenti si impegneranno a:

- utilizzare la rete nel modo corretto
- formare gli studenti all'uso della rete
- dare consegne chiare e definire gli obiettivi delle attività
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

La scuola si farà carico di tutte le precauzioni necessarie per garantire agli/lle studenti/esse l'accesso a materiale appropriato, ma allo stesso tempo non sarà responsabile per l'accesso autonomo da parte degli/lle studenti/esse a materiali inadeguati e potenzialmente dannosi trovati online.

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.

Relativamente agli ambienti di apprendimento il nostro istituto si avvale di:

Sede di Vittuone

- Quattro laboratori di Informatica, con 77 PC per gli studenti e 8 PC per i docenti.

- Laboratorio linguistico, con 26 PC per gli studenti e 1 PC per il docente.

- Laboratorio TPS, con 19 PC per gli studenti e 2 PC per il docente.

- Laboratorio di elettronica, con 12 PC per gli studenti e 1 PC per il docente.

- Laboratorio di preparazione fisica, con 3 PC per i docenti.

- Laboratorio di chimica e biologia (locale 34) con due PC portatili per i docenti.

- Biblioteca, con 1 PC

- Aula 15, con 3 PC

- Postazione ricevimento docenti, con 4 PC

- Segreteria didattica, con 5 PC

- Segreteria amministrativa, DSGA, con 1 PC

- Segreteria personale, con 4 PC

- Aule più palestra con 39 PC

- Aula docenti, con 3 PC

- Presidenza, Vicepresidenza, Ufficio Tecnico, con 3 PC

Sede di Corbetta

- Laboratorio di informatica, con 28 PC per gli studenti e 1 PC per il docente.

- Laboratorio odontotecnico, con 1 PC

- Aula docenti, con 3 PC

- Aule: 10 PC

- Segreteria, 2 PC

- Bidelleria, 1 PC

- Laboratorio di metodologia, 1 PC

- Laboratorio CAD/CAM, 1 PC portatile

- Aula di lettura con 1 PC portatile

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.

Il nostro istituto si è dotato di una regolamentazione condivisa e specifica su tali aspetti per la quale si rinvia al Regolamento d'Istituto.

Il nostro piano d'azioni

AZIONI (da sviluppare nell’arco dell’anno scolastico 2023/2024)

- Effettuare un’analisi sull’utilizzo dei dispositivi personali a scuola da parte deglistudenti 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 delpersonale 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.

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

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell’Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell’Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

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.*

L'IIS Alessandrini Mainardi prevede:

- Corsi di formazione/informazione per studenti, genitori e docenti.
- Un'attivita di peer education, attraverso la formazione di un gruppo ristretto di alunni scelti dai docenti e successivamente formati da esperti dell'associazione

MOIGE all'interno del progetto "Giovani Ambasciatori per la cittadinanza digitale contro cyber bullismo e cyber risk" (https://www.moige.it/progetti/cyberbullismo/).

Si vogliono perseguire i seguenti obiettivi:

- Far diventare il gruppo dei "Giovani Ambasciatori" un importante punto di riferimento per i loro compagni di scuola in relazione ad un utilizzo corretto dei dispositivi digitali, della Rete e dei social network.
- 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

---

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).

La scuola intende prevenire il cyberbullismo attuando delle strategie per:

- creare una consapevolezza diffusa sui rischi del fenomeno del cyberbullismo;

- accrescere le capacità di intervento, sia in ottica preventiva, sia di gestione degli episodi già verificatisi;

- approfondire la conoscenza delle tecnologie digitali, del funzionamento del web, delle dinamiche dei social network;

- coinvolgere diversi attori, con particolare attenzione ai genitori, e alle diverse realtà

- aggregative territoriali, per garantire la promozione di azioni di prevenzione e contrasto anche in contesti diversi da quello strettamente scolastico;

- valorizzare le buone prassi già sperimentate;

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.

La scuola intende attuare le seguenti strategie:

- individuare un referente per indirizzo a cui rivolgersi per effettuare la prima segnalazione.
- decostruire gli stereotipi su cui si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità fornendo agli studenti strumenti quali: video, musica, testi, letture specifiche di sensibilizzazione e test finali di analisi degli argomenti trattati.
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network coinvolgendo l'animatore digitale
- favorire una presa di parola consapevole e costruttiva da parte dei giovani anche tramite il progetto del "giornalino scolastico"
- predisporre per gli studenti: box, indirizzo e-mail, modulistica, App YouPol al fine di raccogliere le eventuali segnalazioni.
- fornire schede informative per riconoscere, prevenire e gestire il fenomeno

---

4.4 - Dipendenza da Internet e gioco online

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

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

La nostra scuola presta particolare attenzione ai segnali comportamentali degli studenti e dellle studentesse da cui si può evincere un attaccamento morboso al gioco online o all'abuso di navigazione virtuale, informando preventivamente i genitori e proponendo percorsi rieducativi con i docenti di informatica. Si provvederà a:

- individuare un referente per indirizzo a cui rivolgersi per effettuare la prima

segnalazione.
- predisporre per gli studenti: box, indirizzo e-mail, modulistica, App YouPol al fine di raccogliere le eventuali segnalazioni.
- fornire schede informative per riconoscere, prevenire e gestire il fenomeno

Nella scuola è già presente uno spazio di ascolto e di consulenza gestito da un esperto: sportello psicologico.

4.5 - Sexting

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

Il nostro istituto si adopererà sia per la prevenzione che per l'eventuale gestione di tale fenomeno. Si provvederà a:

individuare un referente per indirizzo a cui rivolgersi per effettuare la prima segnalazione.

- predisporre per gli studenti: box, indirizzo e-mail, modulistica, App YouPol al fine di raccogliere le eventuali segnalazioni.
- fornire schede informative per riconoscere, prevenire e gestire il fenomeno

Nella scuola è già presente uno spazio di ascolto e di consulenza gestito da un esperto: sportello psicologico.

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.

La scuola intende:

- individuare un referente per indirizzo a cui rivolgersi per effettuare la prima segnalazione.
- nei casi di adescamento online più gravi si prevede l'intervento della Polizia Postale, del Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.
- accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità.

Nella scuola è già presente uno spazio di ascolto e di consulenza gestito da un esperto: sportello psicologico.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa

fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - *Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.*

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **"Segnala contenuti illegali"** (Hotline).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

La scuola intende:

- individuare un referente per indirizzo a cui rivolgersi per effettuare la prima segnalazione.
- nei casi più gravi si prevede l'intervento della Polizia Postale, del Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.
- accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità.
- fornire i seguenti strumenti per la segnalazione: sito www.generazioniconnesse.it alla sezione "Segnala contenuti illegali"

(Hotline); i due servizi messi a disposizione dal Safer Internet Centre: “Clicca e Segnala” di Telefono Azzurro e “STOP-IT” di Save the Children.

Nella scuola è già presente uno spazio di ascolto e di consulenza gestito da un esperto: sportello psicologico.

Il nostro piano d'azioni

AZIONI (da sviluppare nell’arco dell’anno scolastico 2023/2024).

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.

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

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

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

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

Comportamenti rientranti nel cyberbullismo così come previsto e disciplinato dalla L. 29 maggio 2017 n. 71:

a) flaming: litigi online nei quali si fa uso di un linguaggio violento e volgare;

b) harasmment: molestie attuate attraverso l'invio ripetuto di linguaggi offensivi;

c) cyberstalking: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la sua incolumità;

d) denigrazione: pubblicazione all'interno di comunità virtuali di pettegolezzi e commenti crudeli, calunniosi e denigratori;

e) Outing estorto: registrazione delle confidenze, raccolte all'interno di un ambiente privato, creando un clima di fiducia, e successivo inserimento delle stesse in un blog pubblico;

f) impersonificazione: insinuazione all'interno dell'account di un'altra persona con l'obiettivo di inviare dal medesimo messaggi ingiuriosi che screditino la vittima;

g) esclusione: estromissione intenzionale dall'attività online;

h) sexting: invio di messaggi via smartphone ed internet, corredati da immagini a sfondo sessuale.

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.

L'I.I.S. "Alessandrimi Mainardi" metterà a disposizione delle studentesse e degli studenti i seguenti strumenti:

- 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 psicologico;
- docente referente per le segnalazioni.

Studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 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.

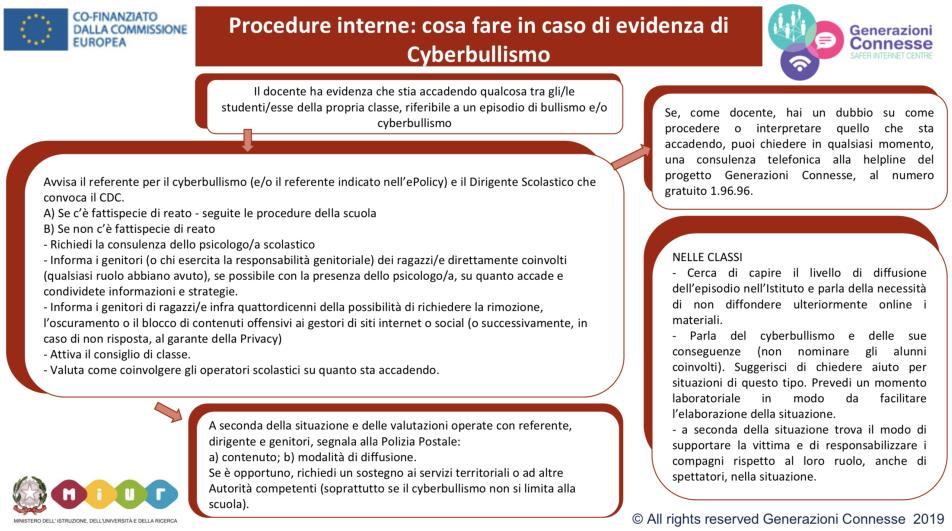
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza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

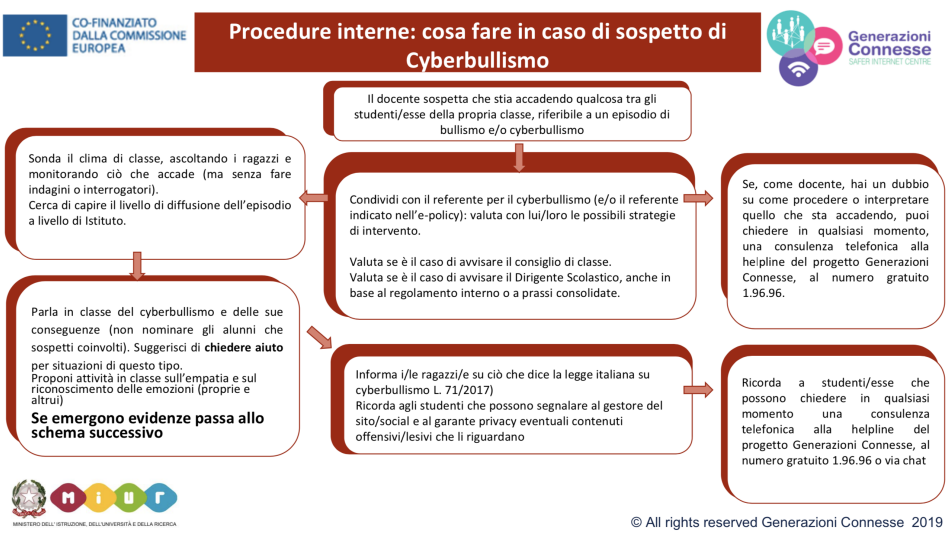
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

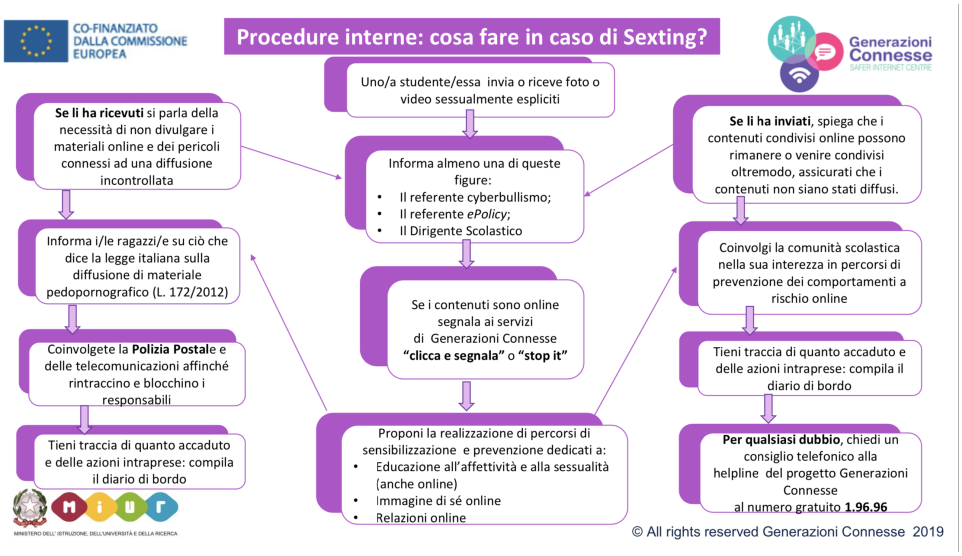
5.4. - Allegati con le procedure

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

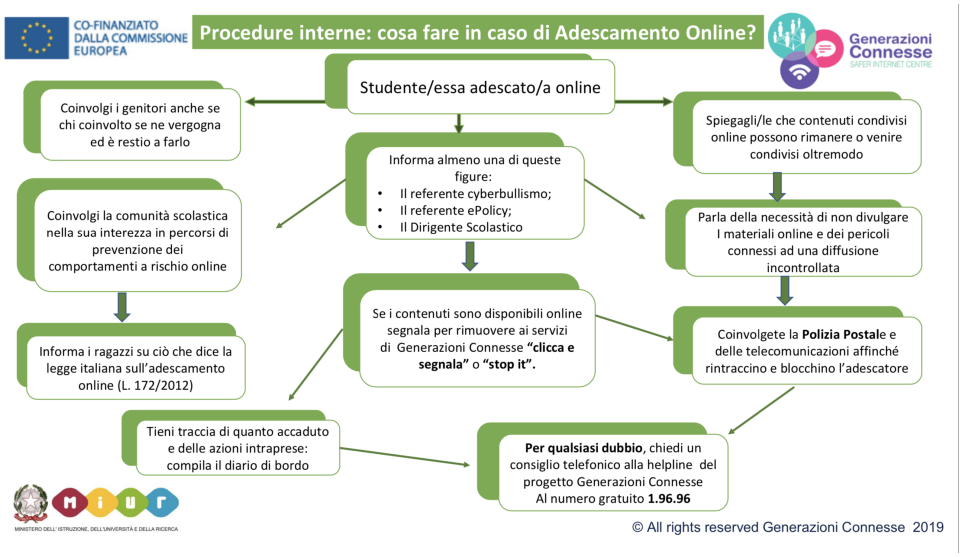




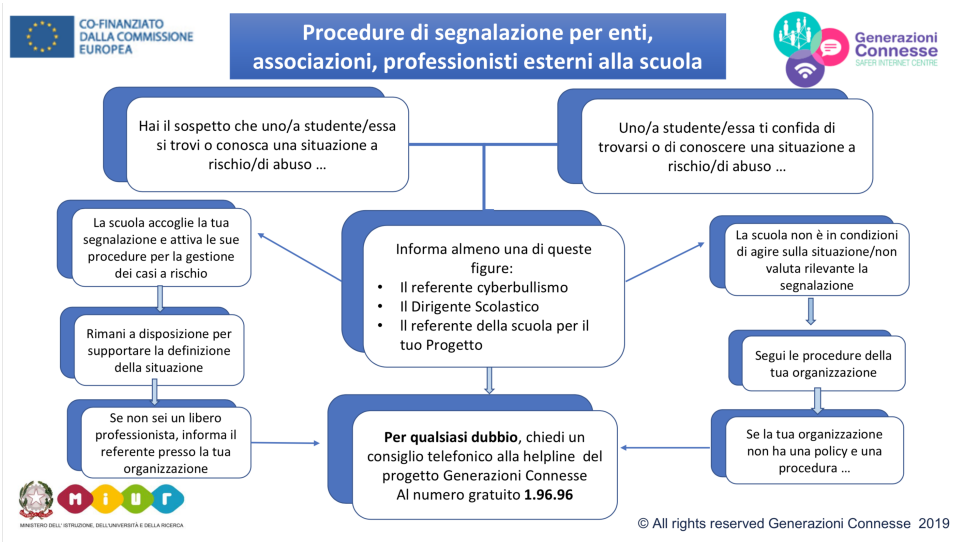
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

Sulla base delle Linee Guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole, vengono assunti i seguenti punti quali indicatori di co-costruzione tra scuola-famiglia-servizi territoriali, al fine di creare un modello composito e lineare di azioni condivise:

- coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori e personale ATA, per la realizzazione di una autentica comunità educante;

- alleanza educativa tra scuola e famiglia

- interventi educativi ed azioni di supporto, quale prevenzione per eventuali comportamenti a rischio;

- misure preventive specifiche di tutela anche con l'ausilio di attori territoriali, come forze dell'ordine ed ASP per servizi specialistici;

- promozione dell'educazione al rispetto;

- sviluppo del pensiero critico;

- promozione dell'Educazione Civica Digitale.