Documento di ePolicy

ROIC81900G

ROVIGO 4

VIA MOZART 8 - 45100 - ROVIGO - ROVIGO (RO)

PAOLA MALENGO

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

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.

Nell'elaborare questo documento, L'Istituto Comprensivo Rovigo 4, si è ispirato alle "Linee di orientamento per azioni di contrasto al bullismo e al cyberbullismo" del 15 aprile 2015 e successiva nota Miur prot. n. 482, "Linee di orientamento per la prevenzione del bullismo e del cyberbullismo" del 18 febbraio 2021. L'obiettivo che ci si propone è quello di orientare l'approccio educativo alla sensibilizzazione verso le "tecnologie digitali" e il loro utilizzo in ambito didattico nonchè quotidiano. Questo documento fornisce le linee guida per garantire il benessere in rete, e stabilire quali siano le norme di comportamento virtuale, ponendo le basi per azioni formative ed educative, per l'uso consapevole e responsabile delle TIC. Di qui la necessità di dotare la Scuola di una propria E-Policy di E-safety, per gestire le eventuali infrazioni, come integrazione del Regolamento d'Istituto, e soprattutto adeguare le misure per la rilevazione e segnalazione di situazioni di rischio legate ad un uso improprio e scorretto delle TIC.

Tutto il processo di progettazione, gestione e monitoraggio delle iniziative formative, che interessano il presente documento, sarà sviluppato nelle modalità ritenute compatibili a tempi, disponibilità professionali e vincoli economici.

1.2 - Ruoli e responsabilità

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

Il sistema scolastico si basa sulle competenze di ogni ruolo , e funzioni operanti, come di seguito specificate.

IL DIRIGENTE SCOLASTICO

- è garante della sicurezza, anche online, di tutti i membri della comunità scolastica;

- promuove la cultura della sicurezza online attivando, con la collaborazione dell' Animatore digitale e del Referente per il bullismo/cyberbullismo, percorsi di formazione riguardanti la sicurezza, le problematiche connesse all'utilizzo della RETE e l'uso consapevole di internet;
- garantisce l'esistenza di un sistema/protocollo per il controllo interno della sicurezza online;
- gestisce e interviene nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali da parte degli studenti e delle studentesse.

L'ANIMATORE DIGITALE

- fornisce consulenza e informazioni al personale in relazione ai rischi on-line, alle misure di prevenzione degli stessi e alla protezione e gestione dei dati personali;
- Promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica) in linea con i contenuti del PNSD e del piano di azione
  triennale allegato al PTOF;
- in collaborazione col referente bullismo e cyberbullismo promuove percorsi di formazione interna all'Istituto per la sicurezza, le problematiche connesse all'utilizzo della RETE e l'uso consapevole di internet;
- monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola.

IL REFERENTE BULLISMO E CYBERBULLISMO

- avvalendosi delle Forze di Polizia, delle associazioni e degli enti territoriali, coordina iniziative specifiche per: 1) la prevenzione e il contrasto del bullismo e cyberbullismo 2) la sicurezza, le problematiche connesse all'utilizzo della RETE e l' uso consapevole di inernet;
- svolge un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav);
- controlla che vengano applicati i protocolli per la corretta segnalazione e procedura nella gestione di eventuali casi di cyberbullismo.

I DOCENTI

- integrano parti del curricolo disciplinare con approfondimenti sull'uso responsabile delle TIC e della RETE servendosi delle tecnologie digitali nella didattica (LIM o altri dispositivi tecnologici);
- sviluppano le competenze digitali degli allievi facendo in modo che gli stessi conoscano e seguano le norme di sicurezza nell'utilizzo del web sia per attività in presenza sia per attività didattiche extracurricolari;
- comunicano al referente sul bullismo e al Dirigente scolastico, 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;
- segnalano al Dirigente scolastico e ai suoi collaboratori qualunque violazione, anche online, del Regolamento di Istituto secondo la procedura stabilita.

IL PERSONALE ATA

- svolge funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza, connesse alle attività dell'Istituzione scolastica, in collaborazione con il Dirigente scolastico e con il personale docente tutto;
- controlla che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti;
- segnala al Dirigente scolastico e ai suoi collaboratori comportamenti non adeguati e/o episodi di bullismo/cyberbullismo;
- collabora nel reperire, verificare e valutare informazioni inerenti possibili casi di bullismo/cyberbullismo

STUDENTI E STUDENTESSE

- rispettano le norme che disciplinano l'uso corretto e responsabile delle tecnologie digitali, come indicato nel Regolamento di Istituto;
- adottano le regole di e-safety per evitare situazioni di rischio per sè e per gli altri.

I GENITORI

- condividono con i docenti le linee educative relative alle TIC e alla RETE, al Regolamento di Istituto e al patto di corresponsabilità educativa;
- condividono il documento di e-Policy dell'Istituto
- collaborano con i docenti e sostegnono la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- seguono 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;
- fissano delle regole per l'utilizzo del computer e controllano l'uso che i figli fanno di Internet e dello smartphone in generale.

GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI

- osservano le politiche interne sull'uso consapevole della Rete e delle TIC;
- attivano procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda: all'art. 21, comma 8, Legge

15 marzo 1997, n. 59; all'art. 25 della Legge 30 marzo 2001, n. 165; al CCNL in vigore; al D.P.R. 8 marzo 1999, n. 275; alla Legge 13 luglio 2015, n. 107; al Piano Nazionale Scuola Digitale; a quanto stabilito in materia di culpa in vigilando, culpa in organizzando, culpa in educando nel Codice Civile.

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).

Ambiti di applicazione, attività e ruoli:

Le agenzie educative extrascolastiche, e gli esperti esterni coinvolti, a vario titolo, nella realizzazione di progetti ed attività formative, sul breve o/e lungo periodo, dovranno prendere atto di quanto stilato nell'E-policy. In relazione al contratto di commissione, dovranno eventualmente sottoscrivere un'informativa sintetica del documento in questione.

Le attività progettuali o di formazione a carattere seminariale, devono essere preventivamente autorizzate, secondo modalità e criteri concordati con l'Istituto. A tal riguardo, al fine di verificare preventivamente i contenuti oggetto della formazione, i soggetti esterni, coinvolti nei progetti formativi, sono tenuti a fornire un dettagliato programma con narrazione sintetica di quanto proposto, per essere valutato e

successivamente autorizzato dal Dirigente Scolastico.

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.

CONDIVISIONE E COMUNICAZIONE DELLA E-POLICY AGLI STUDENTI E ALLE STUDENTESSE

- all'inizio dell'anno, in occasione dell' illustrazione del Regolamento di Istituto agli alunni da parte dei docenti, verrà presentata la e-policy insieme ai regolamenti correlati e al patto di corresponsabilità;
- tutti gli alunni saranno informati che la rete, l'uso di internet e di ogni dispositivo digitale saranno controllati dai docenti e utilizzati solo con la loro autorizzazione e supervisione.

CONDIVISIONE E COMUNICAZIONE DELLA E-POLICY AL PERSONALE SCOLASTICO (DOCENTI E PERSONALE ATA)

- le norme adottate dalla scuola in materia di sicurezza dell'uso del digitale

saranno discusse dagli organi collegiali e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito istituzionale;
- docenti e personale ATA riceveranno un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili sul sito istituzionale nonchè mediante la partecipazione ad eventuali incontri formativi organizzati dall'Istituto. Tutto il personale deve essere consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile, in caso di utilizzo imprudente.

- Il personale ATA è tenuto a prendere visione dell'E-Policy, in particolare il personale amministrativo, essendo necessaria da parte di tutto il personale dell'Istituto la consapevolezza della delicatezza del trattamento dei dati, secondo quanto previsto dal Regolamento UE n. 679/2016 sulla protezione dei dati (GDPR, General Data Protection Regulation).

CONDIVISIONE E COMUNICAZIONE DELLA E-POLICY AI GENITORI

- le norme adottate dalla scuola in materia di sicurezza dell'uso del digitale saranno rese note alle famiglie tramite pubblicazone del presente documento sul sito istituzionale;
- sarà favorito un approccio collaborativo nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione di incontri scuola - famiglia assembleari, collegiali e individuali;
- al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC potranno essere organizzati incontri informativi per presentare e condividere la presente e-policy.

Il presente documento di E-policy, redatto dalla Commissione bullismo/cyberbullismo e approvato dal collegio Docenti e Consiglio di Istituto, sarà inserito all'interno dell'offerta formativa dell'Istituto (PTOF).

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.

Educare alla "consapevolezza civica" verso un uso responsabile della rete è un dovere di tutta la comunità educante. Per questo motivo, accanto all'educazione verso la competenza digitale, sarà premura della scuola introdurre preventivamente delle

modalità formative, in caso utilizzo imprudente del web, nonché l'introduzione di strumenti educativi, per affrontare conseguenze ed errori legati all'infrazione delle netiquette.

INFRAZIONI DEGLI ALUNNI

L'istituto, qualora si ravvisassero infrazioni all'E-policy nell'uso improprio delle TIC, da parte degli studenti, sarà tenuto ad introdurre delle misure per rinforzare i comportamenti corretti, e riparativi, degli eventuali danni causati. Gli interventi correttivi, ovviamente in rapporto all'anagrafe individuale e alla gravità dell'infrazione, sono previsti in relazione a:

- utilizzo di dati personali o foto senza permesso;
- condivisione di immagini a sfondo sessuale;
- collegamento a siti web non adatti all'anagrafe e non indicati dai docenti;
- furto di proprietà intellettuali (file o video musicali protetti da copyright);
- utilizzo della rete per offese, calunnie utilizzo di immagini o video che siano lesivi alla dignità personale;

In ottemperanza a quanto disposto, i provvedimenti disciplinari da adottare sono i seguenti:

- richiamo verbale;
- informazione/comunicazione ufficiale ai genitori;
- sanzioni previste dal regolamento di istituto;
- convocazione dei genitori da parte del Dirigente Scolastico;
- sospensione dalle lezioni;
- in relazione alla gravità dell'infrazione, saranno eventualmente informate le autorità competenti.

INFRAZIONI DEL PERSONALE SCOLASTICO

Anche il personale docente, amministrativo, tecnico e ausiliario, può incorrere in infrazioni nell'utilizzo delle tecnologie digitali e del web; alcune di queste possono favorire conseguenze negative sull'utilizzo corretto delle TIC da parte degli alunni. Nello specifico sono da considerare non adeguati i seguenti comportamenti:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- carente istruzione preventiva degli alunni sull'utilizzo responsabile delle TIC e del web;
- mancata vigilanza che può favorire anche un utilizzo non idoneo dei dispositivi

mobili tra alunni;
- Insufficienti interventi di contrasto nelle situazioni critiche, volti a segnalare ai genitori, all'animatore digitale e al Dirigente Scolastico;

RESPONSABILITÀ GENITORIALE

In un clima di collaborazione fra scuola e famiglia, sarà rinforzata l'attenzione che i genitori, unitamente al corpo docente, dovranno riservare al monitoraggio riguardo l'utilizzo delle TIC da parte degli studenti; in questo l'animatore digitale fungerà da snodo di collegamento per fornire ai genitori indicazioni e consigli per un uso sicuro delle tecnologie digitali; per quanto riguarda i genitori dovranno garantire un controllo parentale verso siti web non certificati (giochi, scommesse, deep web), social media con pubblicazione foto e video che possano compromettere il benessere dei propri figli o dei loro compagni ed amici.

L'istituto scolastico sarà a fianco dei genitori anche per rappresentare le condizioni possibili che possono indurre a comportamenti scorretti. Di seguito alcune situazioni non favorevoli;

- piena autonomia concessa al figlio nell'uso del web e/o nell'utilizzo di devices e/o smartphone: su questo aspetto ricordiamo che i contenuti veicolati nel web da parte dei minori è ascrivibile ai genitori o chi per essi;
- disinteresse verso i devices in possesso dei figli, nonché i contenuti che possono essere veicolati;
- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- 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.

In relazione alle infrazioni legate all'utilizzo del web, tutta la comunità educante è tenuta a collaborare con il Dirigente Scolastico al fine di fornire ogni informazione utile per la valutazione del caso, e il necessario avvio del procedimento disciplinare. Ogni azione di carattere procedurale sarà regolata dalla normativa vigente. In relazione ad infrazioni promosse dagli alunni i genitori saranno convocati, informati sui fatti, e coinvolti nel concordare misure educative correttive, in base alla gravità delle violazioni rilevate.

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.

Le nuove tecnologie sono parte integrante del processo educativo; nel riconoscere questa evidenza il nostro istituto vuole, attraverso questo documento, dotarsi di un approccio programmatico volto a stabilire delle regole e misure di comportamento comuni, connesse in modo particolare all'uso consapevole e responsabile delle tecnologie informatiche.

Dal momento che la scuola tutta è orientata verso il concetto di "una comunità di pratiche", e la normativa vigente va in questa direzione, l'istituto intende con questo documento, rafforzare la conoscenza, nonché i principi che sottendono al rispetto delle regole, con finalità di formare cittadini responsabili e attivi, valorizzando i principi insiti nella Costituzione. Mai come in questo momento storico l'educazione alla cittadinanza digitale risulta dirimente e fondamentale.

L'educazione civica in questo momento deve vigilare sulla rete, che unisce ogni ambito e ogni settore di tutto il processo educativo (linee guida adottate in applicazione della legge 20 agosto 2019 n. 92, e richiamate anche Nell'Agenda 30 ONU), e, nel contesto digitale deve essere garante di diritti di legalità, coerenza e responsabilità.

In questo documento l'istituto descrive gli approcci e le modalità con cui si rivolge alle tecnologie; le misure che vengono utilizzate per la protezione dei dati che corrono in rete, le norme di comportamento da utilizzare da parte dei fruitori dei servizi informatici, le informazioni veicolate dalle TIC in ambito scolastico nonché le problematiche che ne possono derivare.

Nel dettaglio ricordiamo gli obiettivi dell'educazione alla cittadinanza digitale (Legge 20.08.2019 n. 92 art. 5)

- Selezione e affidabilità di fonti, dati, informazioni e contenuti;
- Competenze nell'uso di tecnologie digitali e varie forme di comunicazione;
- Utilizzo servizi digitali pubblici e privati;
- Partecipazione e cittadinanza attiva;
- Netiquette (regole di comportamento nel mondo digitale);
- Strategie di comunicazione;
- Rispetto della diversità;
- Gestione e protezione di dati personali e della propria identità digitale (conoscenza di normative e tutele);
- Benessere psicofisico, individuazione di dipendenze o abusi (cyber bullismo).

Il nostro Istituto nel redigere questo documento fa espressamente richiamo ai contenuti del regolamento d'istituto e in modo particolare al Patto di corresponsabilità educativa in adozione dal 27/06/2019 deliberato dal Consiglio di Istituto con delibera

n. 80.

Per l'istituto il patto di corresponsabilità educativa rappresenta lo strumento cardine d' interrelazione fra scuola e famiglia. Il patto in questione è "contratto educativo" che richiama alla responsabilità tutti gli attori coinvolti nel processo educativo.

Incipit del Patto di corresponsabilità educativo dell'Istituto Comprensivo.

"La scuola è l'ambiente di apprendimento in cui promuovere la formazione di ogni alunno, la sua interazione sociale, la sua crescita civile. L'interiorizzazione delle regole può avvenire solo con una fattiva collaborazione con la famiglia; pertanto la scuola persegue l'obiettivo di costruire un'alleanza educativa con i genitori. Non si tratta di rapporti da stringere solo in momenti critici, ma di relazioni costanti che riconoscano i reciproci ruoli e che si supportino vicendevolmente nelle comuni finalità educative. Impegno di tutti, docenti, alunni, famiglie e personale ATA è quello di favorire un ambiente di lavoro sereno, nel quale possano svolgersi processi di maturazione umana e culturale, per fare, degli alunni di oggi, uomini e donne di domani tutti pienamente inseriti nel mondo e capaci di guardare all'altro con rispetto e solidarietà (DPR 245/2007)".

Il documento che più trova affinità con E-policy è il Regolamento di Istituto, che nasce dall'esigenza, attraverso norme e regole, di garantire un corretto funzionamento all'interno della comunità scolastica, anche quando si tratta della comunità scolastica virtuale.

I regolamenti destinati allo scopo di cui si è fatto accenno sono visibili e consultabili nel sito dell'istituto https://www.icrovigo4.edu.it/.

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.

Data l'importanza che l'Istituto riconosce al presente documento, il monitoraggio e il suo aggiornamento sarà curato dal Dirigente scolastico coadiuvato dall'animatore digitale, dalla funzione strumentale per le nuove tecnologie digitali, dal referente il

bullismo e cyberbullismo e dagli organi collegiali in relazione alle competenze per gli aspetti considerati.

Anche i docenti saranno coinvolti nel monitoraggio del presente documento, allo scopo di verificare l'impatto che l'E-policy ha su tutta la comunità educante.

Il monitoraggio e l'implementazione saranno programmati periodicamente per apportare eventuali miglioramenti in relazione a formazione, interventi educativi, e misure di sicurezza relative all'utilizzo delle nuove tecnologie informatiche.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto agli studenti

Azioni da svolgere nei prossimi 3 anni:

Organizzare un evento di presentazione e conoscenza dell'ePolicy 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.

Le competenze digitali, e la loro applicazione in ambito scolastico, non possono restare all'interno di uno specifico ambito disciplinare, ma devono diventare lo snodo di collegamento fra tutte le aree disciplinari coinvolte nel processo didattico-educativo. Gli studenti devono avere la possibilità di sviluppare gli approcci alle tecnologie digitali, al fine di consolidare la loro competenza in questo ambito, e la scuola, per quanto la riguarda, deve mettere in campo strategie educative per affrontare le nuove modalità di comunicazione ed interazione.

La sfida educativa, da parte della scuola, sta nel portare avanti dei percorsi che mirino a promuovere una consapevolezza digitale, verso l'uso responsabile delle nuove tecnologie.

Il nostro Istituto, partendo dalle indicazioni contenute nel PNSD, ha provveduto all'interno del suo curricolo delle competenze, di individuare dei framework relativi

alle tecnologie digitali che vanno a sostenere:

- L'informazione;
- La comunicazione;
- La sicurezza;
- L'attenzione ai contenuti veicolati;
- Protezione dei dati personali;
- Identificare i bisogni "informatici" espressi dalla comunità scolastica;
- Protezione di "naviganti" della rete, in relazione a: frode, minacce, furti di identità, e cyberbullismo. Questo ultimo punto è stato ampiamente trattato nell'integrazione del regolamento di Istituto (approvato con delibere: n. 17 C.D del 17/05/2019 e n. 80 del C.d.I del 27/06/2019).

Pertanto, le azioni possibili che questo Istituto si propone di fare in merito alle competenze digitali sono:

- Programmare attività per l'uso consapevole delle TIC;
- Sviluppare consapevolezza riguardo l'impatto che possono avere le TIC nella vita delle persone;
- Rappresentare le conseguenze dei comportamenti scorretti all'interno della rete;
- Comprendere quale sia la modalità adeguata quando si utilizza l'ambiente on line;
- Discriminare nel modo adeguato e corretto contenuti e informazioni;
- Conoscere le conseguenze, anche disciplinari, quando si utilizza la rete in modo scorretto;

Tutte le iniziative elencate e intraprese dall'Istituto sono rapportate ai cicli di apprendimento nonchè alle competenze possedute dagli studenti e/o personale docente e non.

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 formazione continua è la base dell'attività educativa e didattica. Per questo il nostro Istituto, che comprende l'importanza della formazione, ritiene fondamentale che tutti i docenti siano formati ed aggiornati, in modo costante e adeguato sui rischi on line. I momenti formativi saranno programmati, in collaborazione con il personale dedicato interno all'istituto (animatore digitale, referente bullismo e cyberbullismo), nonché con personale esterno qualificato, afferente alla rete di scuole, organismi del terzo settore e comparti istituzionali (forze dell'ordine).

A fronte di ciò, consapevoli che la formazione non deve essere esaustiva ma bensì in relazione alla rapida evoluzione delle tecnologie digitali, il nostro istituto dichiara l'intenzione di prevedere momenti di formazione personale e collettiva, anche a distanza.

Allo scopo, il Dirigente Scolastico, coadiuvato dall'animatore digitale, e dalle funzioni strumentali nominate, si propone di raggiungere gli obiettivi specificati nonché indicati nel PNSD (Piano Nazionale Scuola Digitale).

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.

Dal momento che la rete risulta essere un tessuto sociale interattivo comune ad una

vasta platea di persone, la scuola tutta, deve impegnarsi a programmare/progettare percorsi formativi, volti a sviluppare le competenze digitali; allo stesso tempo deve educare gli studenti e le studentesse ad un uso responsabile e consapevole del web. Oramai le competenze digitali sono contemplate dalle indicazioni nazionali ritenute anche dall'Unione Europea competenza chiave trasversale a tutte le discipline. Padroneggiare con abilità le nuove tecnologie digitali non significa solo avere "maggiori competenze" ma soprattutto essere responsabili dell'utilizzo che se ne può fare, nel rispetto degli altri e consapevoli dei rischi e pericoli che si possono causare.

Per sostenere questa visione l'Istituto ha investito sulla formazione digitale dei docenti, collegata con l'educazione alla cittadinanza e alla legalità, , che risultano essere aspetti fondamentali per chiunque utilizzi il web.

Nello specifico l'Istituto si propone l'intenzione di:

- Organizzare percorsi formativi rivolti a tutta la comunità educante;
- Attività e laboratori sulla sensibilizzazione verso l'utilizzo corretto consapevole e responsabile del web, anche in collaborazione con agenzie extrascolastiche e rappresentanze delle istituzioni (Forze dell'ordine);
- Visione di documentari a tema, che rappresentino la gravità e la complessità dei rischi che si nascondono nella rete.

Nel sito dell'Istituto saranno consultabili da parte dei docenti, approcci teorici riguardo l'utilizzo consapevole del web; sarà altresì possibile dal sito istituzionale scolastico accedere al link di "Generazioni Connesse".

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

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

Il “Patto Educativo di Corresponsabilità” fra scuola e famiglia è il sigillo di una alleanza che non si esaurisce con la semplice modalità informativa, ma rappresenta una nuova modalità di coinvolgimento dell’intera comunità educante, che si sente partecipe nel processo formativo di ogni persona. Per il nostro Istituto la scuola e la famiglia sono i protagonisti dell’educazione dei ragazzi, e per questo, diventano alleati negli scambi comunicativi e relazionali. Anche il legislatore ha reso più esplicita questa necessita, prevedendo nell’art. 3 del D.P.R. n° 235 del 21/11/2007, quanto sia fondamentale instaurare un’alleanza forte fra istituzione scolastica e rete familiare. Nel patto di corresponsabilità sono richiamati i principali diritti e doveri che implicano necessari impegni e responsabilità.

Il patto di corresponsabilità, essendo l’espressione di una visione significativa ben più ampia di una realtà dinamica, si propone di essere il documento finalizzato alla costruzione di reti fra istituzione e ambito genitoriale, con tensione ai bisogni educativi di ogni studente. Per questo il nostro Istituto, sensibile ai bisogni di ogni alunno, si propone di fornire un servizio attento e qualificato dal punto di vista didattico-educativo, nonché culturale e relazionale, insistendo sulla capacità dell’Istituto, di perseguire obiettivi formativi significativi a favore della crescita armoniosa degli studenti. All’interno di questo patto di corresponsabilità, sarà data particolare importanza ai rischi connessi all’uso delle TIC, come sarà richiamata la responsabilità di tutti gli attori coinvolti nel processo educativo in relazione a ruoli e competenze. L’istituto sarà garante dell’informazione in tema di tecnologie digitali, previste dall’E-policy, come sarà cura dello stesso aggiornare il Regolamento d’Istituto, il Patto di Corresponsabilità, riguardo le sezioni dedicate alle TIC, sia la pagina web dell’Istituto.

A tale scopo, attraverso la figura dell’animatore digitale e del Referente per il cyberbullismo, l’Istituto attiverà iniziative per sensibilizzare le famiglie riguardo l’utilizzo responsabile della rete e rischi connessi. Per ogni grado di istruzione, l’Istituto consiglia alla funzione genitoriale di monitorare il comportamento virtuale dei figli per evitare rischi on line connessi a condotte non responsabili. I genitori saranno supportati da materiali di approfondimento e approcci teorici forniti dalla scuola, reperibili anche nel sito istituzionale (https://www.icrovigo4.edu.it/) e indirizzati a siti specializzati dotati di aree dedicate, anche in relazione all’anagrafe dei fruitori. L’Istituto consiglia altresì la consultazione della piattaforma Generazioni Connesse e siti istituzionali della polizia di stato.

La comunità scolastica, tutta, deve attenersi a quanto previsto e stabilito nel Regolamento di Istituto e nel Patto di Corresponsabilità Educativa e successive modifiche.

Il nostro piano d'azioni

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

Condividere con il collegio la definizione del curricolo sulle competenze digitali.

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

Organizzare incontri con esperti per i docenti sulle competenze digitali.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

La rapidità dell'evoluzione tecnologica, la globalizzazione, la condivisione e la raccolta di dati personali, hanno comportato nuove sfide per quanto riguarda la protezione dei dati personali.

L'Istituto per migliorare la sicurezza e la protezione dei dati vuole adottare ogni sorta di misura per rispettare le indicazioni normative contenute nel Regolamento Generale per la Protezione dei Dati Personali n. 2016/679 (GDPR), ossia la normativa europea in materia di protezione dei dati.

Il GDPR (General Data Protection Regulation) introduce come principale novità la centralità del principio di responsabilizzazione (accountability), e pone con forza l'accento sulla responsabilizzazione di titolari e responsabili dei dati, ossia l'adozione di comportamenti proattivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

Oggetto e Ambito di applicazione delle misure da adottare per la protezione dei dati:

- Protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
- Trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Finalità perseguite dall'Istituto a sostegno della normativa vigente, ispirandosi ai seguenti principi generali:

- Il principio di necessità: tutti i trattamenti e le tecnologie impiegate tendono alla riduzione dell'utilizzo dei dati personali e identificativi;
- I dati e i relativi trattamenti sono acquisiti ed effettuati esclusivamente per le finalità istituzionali dell'Istituto;
- Tutti i trattamenti previsti eseguiti avvengono in ottemperanza alla normativa vigente;
- Il principio di correttezza e lealtà riguarda la garanzia sia della fedeltà dei dati che dell'integrità nelle modalità di raccolta, archiviazione e trasmissione;
- Sicurezza e protezione: i dati personali sono accessibili solamente al personale preposto e incaricato.

Definizione di dato: "qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

Tipologia di dati:

- Dati sensibili: rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale; i dati relativi alla salute e alla vita sessuale sono detti “super-sensibili”.
- Dati comuni: tutte quelle informazioni idonee a rivelare informazioni, come nome, cognome, codice fiscale, partite I.V.A, indirizzo, posta elettronica, numero di telefono, numero patente, e documento di identità.
- Dati giudiziari: informazioni idonee a rivelare provvedimenti in materia di casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reati o carichi pendenti.

Soggetti responsabili del trattamento.

- Il titolare del trattamento: persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali (art. 4 GDPR). Per la comunità scolastica il titolare del trattamento è l’Istituzione scolastica stessa, nella figura del Dirigente Scolastico.
- Il responsabile del trattamento: la persona fisica o giuridica, distinta dal titolare, che elabora dati per conto del titolare; la nomina del responsabile è regolata da una procedura giuridica.
- Incaricato: la persona fisica autorizzata dal titolare o dal responsabile a compiere materialmente il trattamento.
- L’interessato: la persona fisica a cui si riferiscono i dati stessi.

Trattamento dei dati nella comunità scolastica: l’istituzione scolastica può trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa di settore. Alcune categorie di dati personali degli studenti e delle famiglie – come quelli sensibili e giudiziari – devono essere trattate con estrema cautela, nel rispetto di specifiche norme di legge, coniugando pertinenza e completezza dei dati con la necessaria e indispensabilità dell’interesse che si intende perseguire.

Studenti e famiglie informate: l’Istituto ha l’obbligo di far conoscere agli “interessati” (comunità scolastica, famiglie, docenti) come vengono trattati i loro dati personali. Devono, cioè, rendere noto, attraverso un’adeguata informativa, quali dati raccolgono, come li utilizzano e per quale finalità. Nello specifico, sul sito d'Istituto, nella sezione INFORMATIVE GDPR (menù a sinistra intitolato L'ISTITUTO) si possono visionare le informative sul trattamento dati per i diversi interessati, al seguente link:

https://www.icrovigo4.edu.it/index.php?option=com_k2&view=item&layout=item&id=678&Itemid=232

Diritto di accesso ai dati personali: anche in ambito scolastico, ogni persona ha diritto di conoscere informazioni che la riguardano e di apprenderne il contenuto; per

esercitare questo diritto è possibile rivolgersi direttamente al "titolare del trattamento", l'istituto scolastico, nella persona del Dirigente Scolastico o suoi incaricati.

In ambito scolastico, più che mai, la protezione dei dati oltre che soddisfare i criteri della normativa vigente deve sviluppare consapevolezza del significato della "data protection", in virtù del target di riferimento (minori e non) e le problematiche ad esso collegate, e alla trasformazione continua di una società che è sempre più social e virtuale.

Proprio in ragione di questa trasformazione sociale, la sicurezza informatica diventa un elemento dirimente e fondamentale, e a tal proposito, il MIUR, specifica: "La sicurezza informatica (…) ha lo scopo di minimizzare i rischi che incombono sulle informazioni digitali (non solo sui dati personali in essi contenuti) andando a perseguire il raggiungimento di tre obiettivi: la confidenzialità (o, come l'abbiamo definita in precedenza, riservatezza), l'integrità e la disponibilità delle informazioni. La triade composta da confidenzialità, integrità e disponibilità delle informazioni (in inglese indicata con l'acronimo CIA, per Confidentiality, Integrity e Availability) rappresenta, quindi, il fulcro della sicurezza. La "confidenzialità" si riferisce a quell'insieme di regole che consentono di mantenere il controllo sull'accesso a determinate informazioni escludendo i soggetti non legittimati. Con il concetto di "integrità", invece, ci si riferisce alle regole finalizzate a far sì che le informazioni i dati e documenti siano trattati in modo da prevedere, prevenire e ripristinare i sistemi informatici a seguito di eventi accidentali o volontari in grado di compromettere o alterare indebitamente i sistemi o i dati in esso contenuti. La "disponibilità", infine, si riferisce alle regole e agli accorgimenti attraverso i quali mantenere i sistemi informatici e telematici costantemente operativi, affidabili, funzionali e accessibili."

L'Istituto per migliorare la sicurezza informatica utilizza sistemi di filtraggio e un tipo di proxy per garantire la protezione dei dati trattati, oltre all'aggiornamento periodico del sistema operativo della segreteria che permette la crittografia dei dati.

Ogni informativa sul trattamento dei dati è consultabile nel sito dell'Istituto.

https://www.icrovigo4.edu.it/.

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*

3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

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

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

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

La comunità scolastica, in virtù della continua trasformazione sociale, e di una società sempre più virtuale e connessa, si trova ad affrontare notevoli cambiamenti sia di tipo operativo, per quanto riguarda il decentramento informatico, sia per l'aspetto didattico orientato verso un uso protesico e intelligente della tecnologia. La connessione "always on ", pone l'accento sulle varie problematiche legate alla sicurezza della rete e la conseguente protezione dei dati che al suo interno sono custoditi.

Risorse informatiche utili per le esigenze operative del servizio dell'istituto:

- Dispositivi tecnologici (computer, devices, terminali, linee di comunicazione);
- Sistemi operativi, e/o software;
- Programmi applicativi o memorie esterne;
- Database per i quali si richiede riservatezza integrità e disponibilità.

Le infrastrutture informatiche raggiungono tutte le aule dell'istituto, sono dotate di PC

portatili a diposizione dei docenti, sia per attività formale (compilazione del registro elettronico) che per attività didattica. I dispositivi informatici sono protetti da password e il loro utilizzo è riservato ai docenti. La connessione alla rete wi-fi, finalizzata allo scopo didattico, è riservata al personale docente, e si accede solo attraverso una password.

Politiche di sicurezza modulabile promosse dall'Istituto:

- Chiunque, dipendente o persona esterna, utilizzi risorse informatiche dell'istituto deve essere autorizzato da un responsabile;
- Le autorizzazioni devono garantire la riservatezza delle informazioni;
- L'impiego di persona esterna all'istituto per risorse informatiche deve essere individuabile (cartellino riconoscimento);
- Predisposizione di procedure tecniche organizzative per il sollecito riguardo possibili guasti o malfunzionamenti;
- Utilizzo di filtri e software che impediscano il collegamento a siti inadeguati.;
- Protezione attraverso un uso consapevole delle password;
- L'istituto si impegna a fornire dispositivi sicuri e protetti;
- Per ogni dispositivo è possibile effettuare installazioni e aggiornamenti software;
- Per acquisire una maggiore competenza sull'uso delle tecnologie l'istituto promuoverà attività di formazione per il personale docente e di segreteria.

IL PERSONALE DOCENTE E NON DOCENTE

Il personale docente dell'istituto e/o personale di segreteria è autorizzato alla connessione internet tramite devices personali o forniti dall'Istituto, per attività didattiche, di servizio e/o formative.

Nello specifico:

- Internet può essere usato solo per scopi istituzionali e per quanto riguarda l'ambito professionale;
- Il fruitore è responsabile, civilmente e penalmente, per l'utilizzo del servizio internet, come regolata dalla normativa vigente;
- È vietato inserire nei devices dell'istituto programmi non autorizzati e/o scaricare o installare software non leciti (senza licenza).

Comportamenti adeguati alla professione

- Non è opportuno utilizzare durante le lezioni, da parte dei docenti, telefoni cellulari, se non per scopi previsti istituzionalmente o per integrare le attività didattica;
- L'utilizzo dei dispositivi interattivi all'interno delle classi è subordinato alla responsabilità del docente;
- Gli studenti possono utilizzare devices all'interno della scuola in coerenza con le attività didattiche e sotto la guida e supervisione del docente;

- All’interno dell’istituto la rete internet non può essere utilizzata per scopi diversi da quelli strettamente collegati alle attività didattiche;
- L’uso di fotocamere e registratori audio/video collegato alla rete non è consentito se non autorizzato, ai sensi della normativa vigente;
- Tutti i fruitori del servizio informatico sono tenuti al rispetto delle regole di correttezza e copyright, per quanto riguarda la proprietà intellettuale, del materiale a vario titolo consultato;
- Ogni fruitore è responsabile dell’utilizzo dei dispositivi informatici a lui affidati ed utilizzati per scopi didattici e/o professionali;

Azioni previste per la sensibilizzazione nell’utilizzo delle TIC

Oggi la socialità corre sul web e i così detti nativi digitali, non essendo adeguatamente informati, possono essere i potenziali bersagli della rete, ignari dei pericoli e delle relative conseguenze. Per questo motivo è assolutamente necessario formare tutta la comunità educante sull’utilizzo consapevole di internet e delle nuove tecnologie.

Allo scopo l’Istituto si impegna ad organizzare incontri formativi per i docenti e tutta la comunità scolastica, sull’utilizzo consapevole di internet. I docenti saranno impegnati a favorire momenti di riflessioni con gli alunni sui possibili rischi connessi all’impatto che hanno le nuove tecnologie sulle relazioni sociali.

COMPORTAMENTO ADEGUATO AL PERSONALE ATA DI SEGRETERIA:

Ai sensi della normativa vigente in materia di protezione dei dati personali (Regolamento UE n. 679 del 2016), l’Istituto garantisce che tutti i trattamenti dei dati personali forniti, sono effettuati con correttezza e trasparenza, per fini leciti, tutelando la riservatezza per adempiere ai vigenti obblighi scolastici, amministrativi, contabili e/o fiscali. I dati trattati dall’Istituto vengono comunicati solo in adempimento degli obblighi di legge. Il trattamento illecito dei dati personali prevede pene accessorie secondo la normativa vigente. La specificazione di questa indicazione è fondamentale dato lo snodo essenziale ricoperto dall’area amministrativa. Al personale afferente al ruolo specificato sarà garantita adeguata formazione.

SITO WEB DELL'ISTITUTO

Il sito istituzionale è raggiungibile all’indirizzo: https://www.icrovigo4.edu.it/.

Il Dirigente Scolastico, e chi per esso incaricato, verificano i contenuti destinati alla pubblicazione, a garanzia del trattamento dei dati in base alla normativa vigente.

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.

Nell'epoca della realtà virtuale, le tecnologie rappresentano uno strumento fondamentale a sostegno dell'innovazione didattica. Le TIC rispondono alla complessità globale e creano ambienti di apprendimento capaci di produrre stimoli relazionali, comunicativi e inclusivi; le tecnologie, quindi, a servizio dell'innovazione didattica.

Per questo il nostro Istituto, consapevole dell'importanza che le nuove tecnologie hanno nella vita di ogni studente e docente, ritiene fondamentale rinnovare l'idea della scuola che si evolve da scuola dell'insegnamento a scuola dell'apprendimento.

La rete rappresenta uno spazio interattivo che può aprire proficue modalità di dialogo, nello specifico:

- La dimensione multimediale che ci permette la rete riguarda sia la vicinanza con gli studenti ma soprattutto l'interazione didattica fra discipline diverse;
- Le risorse informative che ci offre la rete in qualunque momento, e per qualsiasi argomento;
- La rete come mezzo inclusivo per una platea di attori che necessitano di utilizzi protesici (sintetizzatori, siti interattivi, canali per software didattici specifici per l'apprendimento);
- Risorse destinate all'aggiornamento professionale del corpo docente;
- Siti di istituto, come strumenti ad alta visibilità, per informare, per essere competitivi, e per raggiungere una platea su larga scala;
- La comunicazione globale diminuisce le distanze e favorisce la realizzazione di progetti comuni anche a distanza;
- L'interesse delle giovani generazioni verso l'interazione virtuale;
- L'educazione a distanza fruibile in ogni momento con analoghe modalità dell'educazione in presenza;
- Utilizzo della rete per la diffusione e condivisione di informazioni e notizie da parte dei siti ministeriali.

L'utilizzo degli strumenti multimediali per scopi didattici, con il richiamo a collegamenti di ipertesto e/o ipermedia, favorisce la creazione di scenari individualizzati e/o personalizzati, scegliendo di volta in volta gli strumenti più adeguati per coniugare gli obiettivi didattici agli obiettivi da raggiungere.

La consuetudine nell'utilizzo della rete consente di inserire contenuti didattici all'interno di una platea aperta e vasta; l'educazione on line permette di adottare modalità sincrona e a-sincrona, e spaziare fra tutti i contenuti messi a disposizione

dalla rete sotto forma di pagine web. Ovviamente non dobbiamo pensare che la rete renda obsoleti gli altri mezzi di trasmissione dei contenuti didattici: la didattica digitale deve essere integrata con la didattica tradizionale.

Il nostro istituto, sotto questo profilo, ha dato ampio respiro al sito web istituzionale, chiaro, con ampia visibilità e di facile consultazione, oltre ad altri spazi virtuali all'interno dei quali la comunità educante si confronta.

1. Piattaforma virtuale dell'istituto:

- Piattaforma G Suite for education (per la didattica integrata e a distanza) con applicazioni per la didattica, tra cui Classroom per l'interazione didattica studenti e docenti per modalità sincrona e asincrona;

2. Portale elettronico che permette di

- Registrare presenze di docenti e studenti;
- Consultare il registro elettronico in merito alla programmazione quotidiana didattica
- Bacheca web per tutte le comunicazioni ufficiali che interessano la vasta platea dei docenti;
- Agenda web per annotare e consultare impegni ed eventi istituzionali;

3. Casella di posta elettronica istituzionale personale per comunicazioni ufficiali.
4. Le chat informali create per scopo professionale e didattico; dal momento che non esiste una vera e propria regolamentazione, a tal riguardo si richiama ad una riflessione riguardo l'utilizzo dello spazio interattivo, nonché la condivisione di regole di buon senso destinate alla regolamentazione degli accessi virtuali.
5. Il Sito istituzionale prevede un'area pubblica per la consultazione di informazioni che non veicolano dati riservati, destinata alla consultazione di iniziative, progetti, scadenze temporali e avvisi generali.

Tutte le piattaforme virtuali sono accessibili attraverso il riconoscimento mediante password fornita dalla segreteria amministrativa dell'Istituto; ogni docente avrà il compito di custodire e salvaguardare le credenziali ricevute.

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 Piano Nazionale Scuola Digitale è un pilastro fondamentale su cui si basa "La Buona Scuola" (Legge 107/2015), una visione operativa che rispecchia la posizione del Governo rispetto alle più importanti sfide di innovazione del sistema pubblico; al centro di questa visione, vi sono l'innovazione del sistema scolastico e le opportunità dell'educazione digitale.

In questo paradigma, le tecnologie diventano abilitanti, quotidiane, ordinarie, al servizio dell'attività scolastica, in primis le attività orientate alla formazione e all'apprendimento, ma anche l'amministrazione, contaminando - e di fatto ricongiungendoli - tutti gli ambienti della scuola: classi, ambienti comuni, spazi laboratoriali, spazi individuali e spazi informali".

In relazione a questo, le dotazioni informatiche e le infrastrutture presenti all'interno dell'istituto, LIM, PC portatili, TV, memorie esterne, laboratori informatici, vanno utilizzate nel rispetto delle norme contenute e previste nel Regolamento interno dell'Istituto approvato in data 25.05.2016 con delibera n. 126.

I danni causati per negligenza, incuria o frutto di gesti inadeguati da parte di chiunque saranno risarciti dai responsabili. Il danno causato dai minori, previa valutazione della situazione da parte dell'Istituto, sarà risarcito dai genitori.

Tutte le dotazioni e strumentazioni TIC sono fruibili solamente per scopo didattico ed è esclusivamente riservato a docenti e studenti. I docenti hanno il compito di vigilare sull'utilizzo delle infrastrutture multimediali all'interno delle aule e laboratori, ma hanno altresì il compito di formare gli alunni al rispetto delle dotazioni TIC e conseguente applicazione.

I docenti nell'esercizio della professione hanno la possibilità di utilizzare devices per scopi didattici, per integrare la didattica tradizionale o per raggiungere studenti nelle aree virtuali create ed utilizzate.

I docenti possono utilizzare:

- La connessione internet della scuola;
- I PC e Tablet della scuola;
- Lavagne interattive all'interno delle aule scolastiche;
- Devices personali, a scopo didattico.

Gli studenti possono utilizzare:

- I PC e Tablet della scuola - l'utilizzo è funzionale alle attività previste dal docente e subordinato alla supervisione dello stesso.

Norme di comportamento della comunità scolastica.

- È proibito utilizzare fotocamere e registratori audio/video se non autorizzato;
- Non è acconsentito modificare le impostazioni internet tali da compromettere le impostazioni di sicurezza;
- Il docente è responsabile della consultazione on line nell'ambito dell'orario di servizio all'interno della classe;
- La cura delle informazioni condivise sulle piattaforme on line è un dovere di ogni cittadino virtuale;
- Tutta la comunità scolastica è tenuta alle regole della correttezza riguardo la proprietà intellettuale (copyright);
- Tutta la comunità scolastica è responsabile dell'integrità di arredi e attrezzature informatiche di proprietà della scuola.

Comportamenti scorretti da evitare

- Violare la sicurezza di archivi e computers;
- Compromettere il funzionamento della rete e di apparecchi con programmi non leciti e nocivi (virus, Trojan horses …)

L'Istituto raccomanda di adottare quei principi di buon comportamento nell'utilizzo delle TIC, che vanno a corredare i principi fondamentali della netiquette, ossia la buona educazione in rete.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/21).

Promuovere la diffusione di informazioni per sensibilizzare le studentesse e gli studenti dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.

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

Organizzare uno o più eventi o attività volti a formare il personale adulto

dell’Istituto 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.*

Una conseguenza della maggiore disponibilità e facilità di accesso a internet è l'aumento della frequenza e del tempo che adolescenti e preadolescenti spendono online. Le ricerche hanno dimostrato che opportunità e rischi di internet vanno di pari passo: vale a dire, più i ragazzi usano internet, più beneficiano delle opportunità di questo contesto, esponendosi al contempo anche a maggiori rischi. Il fatto che i

ragazzi utilizzino frequentemente le TIC non implica necessariamente che siano consapevoli di tutti i rischi che questi ambienti possono comportare, né tantomeno che siano a conoscenza delle migliori strategie da adottare per far sì che la loro «esperienza online» sia il più possibile sicura e positiva.

Al fine della sensibilizzazione e prevenzione, il nostro Istituto si propone di educare, informare e responsabilizzare gli alunni sui rischi che corrono ogni giorno in Rete, senza demonizzarla, bensì sollecitandone un utilizzo consapevole, in modo che Internet possa rimanere per loro una fonte di divertimento e apprendimento. In questa ottica la nostra scuola intende attivare percorsi di educazione alla legalità e alla cittadinanza digitale, oltre che promuovere le competenze previste dal curriculo digitale.

Un accento particolare viene dato:

- alla conoscenza dell'importanza di tutelare la propria privacy e quella degli altri (dati sensibili, password, foto, video) e dell'implicazioni legali in caso di trasgressione;
- alla conoscenza delle regole o norme etiche da tenere in mente quando si naviga in rete, quando si pubblica e/o si condivide un contenuto;
- alla riflessione di come sia possibile dietro uno schermo, protetti dall'anonimato infrangere con facilità tali norme, essere vittime o artefici di azioni lesive e offensive della propria e altrui persona.

Linee guida per i docenti al fine di prevenire i RISCHI ON LINE

- discutere con gli alunni della policy e-safety della scuola, di utilizzo consentito della rete e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet;
- dare chiare indicazioni su come si utilizza Internet ed eventualmente anche la posta elettronica, e informare che le navigazioni saranno monitorate;
- ricordare di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione su Internet del laboratorio (qualora sia stata attivata);
- ricordare agli alunni che la violazione consapevole della policy e-safety della scuola comporta sanzioni di diverso tipo;
- adottare provvedimenti "disciplinari", proporzionati all'età e alla gravità del comportamento;
- adottare interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni;
- nelle situazioni psico-socio-educative particolarmente problematiche, convocare i genitori o gli esercenti la potestà per valutare con loro a quali risorse

territoriali possono rivolgersi (Servizi Sociali per la fruizione di servizi socio-educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica, Pediatria, Neuropsichiatria infantile, Consultorio Familiare);
- chiedere/suggerire di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indirizzo e-mail, ecc... ;
- segnalare la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale;
- in caso di abuso sessuale rilevato anche attraverso i nuovi mezzi di comunicazione come internet o il cellulare, confrontarsi con i colleghi di classe e il Dirigente Scolastico, denunciare all'autorità giudiziaria o agli organi di Polizia.

Consigli ai genitori per un uso responsabile di internet a casa al fine di prevenire i RISCHI ON LINE

- evitare di lasciare le e-mail o file personali sui computer di uso comune;
- concordare con il proprio figlio le regole: quando si può usare internet e per quanto tempo;
- inserire nel computer i filtri di protezione per prevenite lo spam, i pop-up pubblicitari, l'accesso a siti pornografici;
- aumentare il filtro del "parental controll" attraverso la sezione sicurezza in internet dal pannello di controllo;
- attivare il firewall (protezione contro malware) e antivirus;
- mostrarsi coinvolti: chiedere al proprio figlio di spiegarvi come funziona internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante;
- incoraggiare le attività on-line di alta qualità: ricercare informazioni scientifiche, ricercare nuovi amici nel mondo;
- partecipare alle esperienze on-line: navigare insieme al proprio figlio, discutere gli eventuali problemi che si presentano, ...;
- stabilire ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia);
- discutere sul tema dello scaricare file e della possibilità di ricevere file con virus;
- raccomandare di non scaricare file da siti sconosciuti;
- incoraggiare il proprio figlio nel caso in cui veda immagini particolari o riceva e-mail indesiderate;
- discutere nei dettagli le conseguenze se si visitano deliberatamente siti non adatti, ma non rimproverare se compie azioni involontarie;
- spiegare che le password, i codici pin, i numeri di carta di credito e i numeri di telefono e i dettagli degli indirizzi e-mail sono privati e non devono essere dati ad alcuno;
- spiegare che non tutti su Internet sono chi realmente dichiarano di essere; di conseguenza i ragazzi non dovrebbero mai accordarsi per appuntamenti senza

consultarvi prima;
- il modo migliore per proteggere il proprio figlio è usare Internet con lui, discutere e riconoscere insieme i rischi potenziali.

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).

Sulla base delle differenti modalità in cui avviene l'aggressione on line , sono state individuate 8 diverse categorie di cyberbullismo:

1. Flaming: messaggi online violenti e volgari indirizzati con lo scopo di suscitare vere e proprie battaglie verbali, tra due o più soggetti, all'interno di forum, chatroom e gruppi online.
2. Harassment: messaggi offensivi e molesti inviati ripetutamente alla stessa persona. In questo caso la persona che riceve gli insulti rientra a tutti gli effetti nella categoria di vittima, perché indifesa e del tutto incapace di reagire alle molestie subite;
3. Cyberstalking: ripetuti tentativi di contatto che il molestatore tenta di instaurare con la sua vittima attraverso l'utilizzo dei media digitali.
4. Denigration: diffusione, da parte del molestatore, di pettegolezzi, calunnie e offese all'interno di comunità virtuali allo scopo di danneggiare la reputazione della vittima.
5. Impersonation: vera e propria sostituzione di persona che consiste nel violare l'identità virtuale della vittima con l'obiettivo di darle una cattiva immagine e danneggiarne la reputazione;
6. Trickery: pubblicazione e diffusione di informazioni riservate e/o imbarazzanti estorte alla vittima con l'inganno, dopo aver instaurato con lei un clima di fiducia al solo scopo di danneggiarla;
7. Exclusion: esclusione deliberata di una persona da un gruppo online allo scopo di suscitare in essa un sentimento di emarginazione;
8. exposure: la pubblicazione online di informazioni private e/o imbarazzanti su un'altra
   persona;

L'Istituto Comprensivo Rovigo 4 intende svolgere diverse azioni finalizzate alla prevenzione del Cyberbullismo:

- accompagnare gli alunni nella navigazione in Rete, coinvolgendoli nell'esplorazione delle opportunità e dei rischi, con attività calendarizzate dall'inizio dell'anno;
- approfondire, con attività mirate in classe, la conoscenza del fenomeno del cyber bullismo e della Netiquette, cioè insieme di regole informali che disciplinano il buon comportamento di un utente sul web, specie nel rapportarsi agli altri utenti attraverso risorse come newsgroup, mailing-list, forum, blog, reti_sociali o email in genere;
- creare degli spazi in cui gli alunni si possano confrontare attivamente su questo tema, coinvolgendoli in attività di peer - education e utilizzando come spunti di riflessione spezzoni di film, canzoni, ecc...;
- creare occasioni di confronto tra insegnanti della scuola o con esperti del territorio;

- valutare gli studenti a rischio, osservarne il disagio, rilevarne i comportamenti dannosi per la salute di ragazzi/e;
- formare il personale scolastico, prevedendo la partecipazione ai moduli formativi previsti dalla piattaforma ELISA di uno/due docente/i referente per l'Istituto;
- svolgere attività di informazione rivolte a docenti, studenti, famiglie e personale ATA, sui temi dei regolamenti e delle procedure adottate dal referente per il bullismo e il cyberbullismo e dal Team Antibulllismo;
- svolgere attività di rilevazione dei fenomeni di cyberbullismo attraverso osservazioni costanti da parte di tutto il personale scolastico;
- attivare un sistema di segnalazione nella scuola (vedi scheda allegata);
- attivare, quando possibile, uno sportello psicologico e un centro di ascolto gestito da personale specializzato (psicologi presenti nell'istituto o nei servizi del territorio;
- costituire gruppi di lavoro che includano il/i referente/i per la prevenzione del bullismo e del cyberbullismo, l'animatore digitale e altri docenti impegnati nelle attività di promozione dell' educazione civica per l'aggiornamento del documento di e-Policy d'istituto e del curricolo digitale.

Cosa deve fare un docente nel caso di sospetto cyberbullismo?

Vedi scheda allegata all' E-policy.

Cosa deve fare un docente in caso di evidente cyberbullismo?

Vedi scheda allegata all' E-policy.

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.

- condivisione nei Consigli di Classe di percorsi trasversali di Educazione civica tesi alla promozione dei diritti umani;
- sviluppo delle competenze digitali ed educazione ad un uso etico e consapevole delle tecnologie per la promozione della consapevolezza di queste dinamiche in rete;
- interventi finalizzati a stimolare le abilità emotive ed empatiche degli studenti;
- percorsi di riflessione e responsabilizzazione sull'uso delle parole;
- redazione di decaloghi condivisi dagli alunni al fine di diffondere l'uso di un linguaggio non offensivo, anche avvalendosi del supporto di materiali presenti sulla Piattaforma Generazioni Connesse.

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?

Il nostro Istituto si propone di promuovere la capacità di creare o mantenere una relazione sana con la tecnologia, integrandola nella didattica e mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini on line e dei rischi connessi. In questa ottica si ritiene fondamentale avviare con gli alunni un percorso di riflessione relativo alle criticità connesse all'utilizzo dei videogiochi, che possono essere:

- la dipendenza legata ad un loro uso eccessivo, con il rischio di trascurare lo studio e le relazioni amicali;
- se utilizzati per molte ore, possibili problemi di salute legati all'eccessivo

stress, a disturbi del sonno, manifestazioni di ansia ecc., ma anche il rischio di sviluppare una miopia indotta dall'eccessivo sforzo di messa a fuoco ravvicinata (questo vale in generale anche per il cellulare);
- i rischi di subire violazioni della privacy;
- contatti indesiderati nei casi di videogiochi online;
- esposizione a contenuti potenzialmente dannosi;
- rischio di virus e malware sui dispositivi (a causa di app infette) e di phishing;
- rischi specifici legati al gioco d'azzardo online, inclusa la ludopatia.

Al fine di controllare la tecnologia e di conoscerne le potenzialità, risulta di fondamentale importanza con gli alunni non demonizzare i videogiochi, ma sottolinearne gli aspetti positivi di seguito riportati:

- contribuire allo sviluppo di abilità tecniche e strategiche;
- migliorare la coordinazione oculo-motoria;
- contribuire all'acquisizione di abilità di problem solving.

Avviare percorsi di riflessione sull'uso consapevole del tempo libero e del tempo trascorso on line porterà i ragazzi ad apprezzare il valore che questo tempo aggiunge alla propria vita e li renderà più consapevoli dell'atteggiamento più giusto da tenere quando sono collegati alla rete; strutturare proposte alternative ai videogiochi che abbiano come strumento giochi virtuali d'aula, li aiuterà ad usare il pieno potenziale della tecnologia limitandone i rischi. Si ritiene inoltre fondamentale concordare una linea d'azione condivisa con la famiglia, per stabilire mezzi e modalità durante lo studio domestico, con forme di controllo attivo durante la navigazione in Rete.

4.5 - Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti 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.

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

- discutere con gli alunni delle esperienze relative ad Internet e i nuovi media e mostrare di essere interessati alla loro "vita digitale";
- incoraggiare gli alunni a confidare le cose che li turbano o a rivolgersi a un adulto di cui si fidano;

- affrontare insieme la questione della presentazione di sé su Internet, adeguando l'approccio a seconda del sesso;
- affrontare il tema della pubblicazione di immagini e video che potrebbero diventare pericolosi, se messi in circolazione contro la loro volontà. Consigliare loro di chiedersi sempre se sarebbero contrari a che tali immagini fossero affisse per strada o circolassero sul piazzale della scuola;
- sconsigliare vivamente di inviare, mettere in rete o conservare su supporti privi di protezione fotografie o video che li ritraggono nudi o in pose provocanti o quantomeno consigliare loro di fare in modo di essere irriconoscibili;
- sensibilizzarli sul fatto che non devono diffondere abusivamente immagini di altri: cliccando like o condividendo fotografie o video con terzi si rendono colpevoli di cyberbullismo e contribuiscono ad aumentare la sofferenza della persona ritratta.

Cosa devono fare i docenti nella situazione in cui vengano a conoscenza di un caso di sexting?

Vedi scheda allegata all' E-policy

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.

- Guidare gli alunni nella conoscenza degli aspetti legati alla corporeità e, soprattutto, alla relazione; la sessualità non è e non deve essere un argomento tabù a scuola;
- creare delle attività, dei percorsi o dei laboratori che possano promuovere il senso di fiducia, l'autostima, il riconoscimento di segnali che possono aiutare a instaurare una relazione autentica con gli altri;
- insegnare ai propri alunni (anche attraverso incontri con esperti) come utilizzare le informazioni di sicurezza dei diversi social network che frequentano e ad utilizzare eventuali bottoni di segnalazione o funzioni di blocco dei contatti che li infastidiscono online;
- insegnare ai propri alunni a non fidarsi ciecamente delle persone conosciute online: non tutti sono chi dicono di essere e spesso si possono incontrare malintenzionati;
- avvisare gli alunni che spesso vengono adescati con la scusa di volerli reclutare per pubblicità/casting chiedendo loro foto o video;
- fare ragionare gli alunni sulla pericolosità del diffondere online materiali foto/audio/video in quanto chiunque può scaricare/registrare/archiviare questi materiali, a volte al solo scopo di ricattarli;
- esortare gli alunni a non vergognarsi a chiedere informazioni agli adulti di cui si fidano e a confidare eventuali "brutti incontri online";
- evitare di colpevolizzare l'alunno/a vittima di adescamento;
- creare momenti di confronto su questo tema facendo anche riferimento ai materiali prodotti da altri alunni coinvolti nel progetto SIC – Generazioni Connesse negli anni precedenti.

Cosa devono fare i docenti nella situazione in cui vengano a conoscenza di un caso di supposto adescamento on line?

Vedi scheda allegata all' E-policy.

Indicazioni per i genitori:

- monitorare le attività online del minore per un tempo consistente a partire dal momento in cui gli viene concessa la possibilità di navigare in modo solitario e di gestire autonomamente un proprio profilo sui social network o di utilizzare un proprio indirizzo di posta elettronica. Ciò non implica violare la sua Privacy, ma concordare assieme a lui che periodicamente le figure di riferimento verifichino in sua presenza i contenuti dei suoi post, i messaggi e le immagini che lo hanno visto coinvolto con altre persone;
- fornire aspettative chiare e condivise in relazione ai contatti online di un figlio minorenne, discutendo e definendo con lui limiti e regole di auto-protezione e auto-tutela che dovranno essere rispettate ogni volta che entra in contatto con sconosciuti;
- parlare in modo approfondito dell'adescamento online non per generare

spavento, ma per facilitare la presa di coscienza e di consapevolezza da parte dei ragazzi;

- dare la certezza ai vostri figli che voi siete e sarete sempre disponibili a parlare con loro di tutto, e che anche quando si trovassero nel peggiore dei pasticci e avessero a comunicarvi ciò che hanno commesso o la situazione complicata in cui si trovano coinvolti, voi vi preoccuperete per loro ed eviterete di arrabbiarvi;
- di fronte ad ogni dubbio, non limitatevi a sperare di esservi sbagliati e che probabilmente non è successo niente di grave, ma approfondite sempre la ricerca, in particolare, rispetto a situazioni che non vi sembrano chiare o che non vi lasciano tranquilli.

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.

L'Istituto Comprensivo Rovigo 4, per realizzare una prevenzione efficace, si pone l'obiettivo primario di rafforzare i fattori protettivi, cioè favorire e potenziare tutte quelle condizioni individuali che proteggono un bambino da abusi sessuali. A tal fine la scuola dovrà aiutare l'alunno a discriminare i pericoli, riconoscere le persone con cui entra in relazione e da cui riceve attenzioni affettive, definendone l'appropriatezza delle modalità.

Risulta quindi fondamentale promuovere l'acquisizione di competenze sociali e lo sviluppo del benessere emozionale, affrontandoli trasversalmente durante le attività curriculari. Una corretta prevenzione può avvenire anche all'interno di un più generale programma di educazione sessuale, condizione che la scuola deve assolvere con la dovuta competenza psico-pedagogica, aiutando i bambini a sviluppare una sessualità più consapevole e al contempo mettendoli in guardia senza ipocrisie o terrorismi sui pericoli che derivano dagli abusi sessuali.

È utile ricordare sia al personale scolastico che ai genitori degli alunni le quattro "R", cioè le regole alla base di qualsiasi intervento di prevenzione dell'abuso sessuale:

- riconoscere possibili situazioni di rischio, distinguendole da situazioni innocue;
- reagire al potenziale abuso tramite strategie assertive verbali e comportamentali;
- riferire l'abuso a figure di riferimento di cui ci si fida;
- rassicurare il bambino e l'adolescente nel caso in cui si senta responsabile o in colpa per quanto accaduto.

Il nostro piano d'azioni

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

Promuovere la diffusione di informazioni per sensibilizzare le/gli alunne/i sui rischi online e sull'utilizzo sicuro e consapevole delle tecnologie digitali.

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

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

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.

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile di internet. La scuola, quindi, avrà cura di porre attenzione alla rilevazione di rischi connessi alla navigazione sul web, in modo particolare al cyberbullismo, all'adescamento online e al sexting.
In particolare dovranno essere segnalati:

- contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono,informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

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.

I Docenti sono tenuti a svolgere attività di rilevazione attraverso osservazioni costanti e, qualora si rendano conto di trovarsi di fronte a situazioni di criticità, dovranno rivolgersi ai Referenti, che avvieranno le procedure con le istituzioni preposte, nonché la segnalazione alla Dirigenza Scolastica. Essi avranno a disposizione uno strumento di segnalazione (vedi allegati), sul quale descrivere le situazioni che si verranno a determinare. E' opportuno che il personale della scuola, anche con l'ausilio del personale di assistenza tecnica e dell'Animatore digitale, provveda a conservare le eventuali tracce di una navigazione non consentita su Internet o del passaggio di materiali inidonei sui pc della scuola; la data e l'ora consentiranno di condurre più approfondite indagini; nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. Sia nel caso di chat che di messaggi di posta elettronica, l'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove dell'indagine sugli abusi commessi. Tali prove saranno utili anche ad informare la famiglia dell'alunno vittima di abuso.
In base all'entità dei fatti si provvederà:

- a una comunicazione scritta tramite diario alle famiglie;
- a una nota disciplinare sul registro di classe;
- a una convocazione formale dei genitori degli alunni, tramite segreteria;
- a una convocazione delle famiglie da parte del Dirigente Scolastico.

Per i reati più gravi gli operatori scolastici hanno l'obbligo di effettuare la denuncia

all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti). Inoltre ci si potrà avvalere dei due servizi messi a disposizione dal Safer Internet Center il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children. Una volta ricevuta la segnalazione, infatti, gli operatori procederanno a coinvolgere le autorità competenti in materia.

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.

Qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola è possibile rivolgersi ad enti e servizi presenti sul territorio di cui si forniscono gli opportuni riferimenti:

COMITATO REGIONALE UNICEF VENETO

Cannaregio, 23 - Fondamenta Santa Lucia -
30123 – Venezia

comitato.veneto@unicef.it
Tel: 041 2794393

Fax: 041 2794282

CORECOM
Via Poerio, 34 30171 - Mestre Venezia
041 2701650
corecom@consiglioveneto.it
http://corecom.consiglioveneto.it/corecom/
Competenze/Servizi: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale. Tra le varie attività, particolare attenzione è riservata alla tutela dei minori.

UFFICIO SCOLASTICO REGIONALE
Riva de Biasio S.Croce 1299 30135 - Venezia
041 272 31 11
direzione-veneto@istruzione.it
www.istruzioneveneto.it/wpusr/
Competenze/Servizi: tra le varie funzioni, supporta la scuola in attività di prevenzione. Può affiancare le scuole nei casi di segnalazione di comportamenti a rischio correlati all'uso di internet.

POLIZIA POSTALE E DELLE COMUNICAZIONI

Compartimento Venezia Via Torino, 88
041/2907311
poltel.ve@poliziadistato.it
www.commissariatodips.it/
Competenze/Servizi: si occupa di accogliere tutte le segnalazioni o denunce relative a comportamenti a rischio nell'utilizzo di internet e che si configurano come reati.

AZIENDA SANITARIA LOCALE: ULSS 5 POLESANA

Viale Tre Martiri n. 89 – 45100 Rovigo

0425 3931 (centralino)

urp.ro@aulss5.veneto.it

GARANTE REGIONALE PER L'INFANZIA E ADOLESCENZA

Garante regionale dei diritti della persona
Mirella Gallinaro
Via Brenta Vecchia, 8 - 30171 Mestre (VE)

Tel.: 041 2383422-23
Email: garantedirittipersonaminori@consiglioveneto.it
P.e.c.: garantedirittipersonaminori@legalmail.it

Il Garante conosce, ascolta, consiglia, promuove, si prende cura, nell'ambito del territorio regionale, dei diritti dei minori di età, oltre a quelli dei cittadini nei confronti della pubblica amministrazione e dei diritti delle persone ristrette nelle libertà personali. Il Garante agisce in piena autonomia, secondo procedure non giurisdizionali di promozione, protezione e facilitazione nel perseguimento dei diritti delle persone; non è soggetto ad alcuna forma di controllo gerarchico o funzionale: questo gli garantisce piena libertà di giudizio e di valutazione.

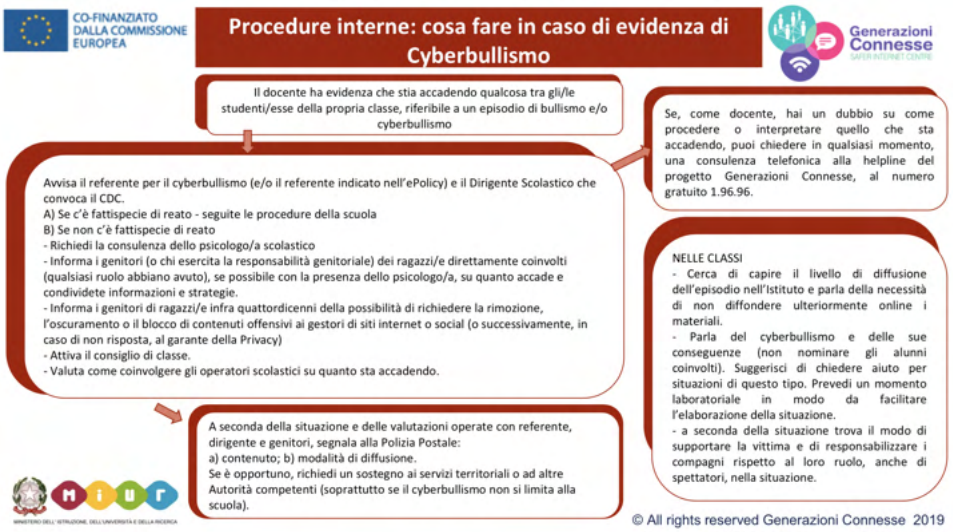
TRIBUNALE PER I MINORENNI
Via Bissa, s.n.c. – Mestre – 37173 - Venezia
041.066212 (centralino)
tribmin.venezia@giustizia.it
www.tribunaleminorennivenezia.it/

Tra le varie attività si occupa di tutti i procedi-menti che riguardano reati, misure rieducative, tutela e assistenza.

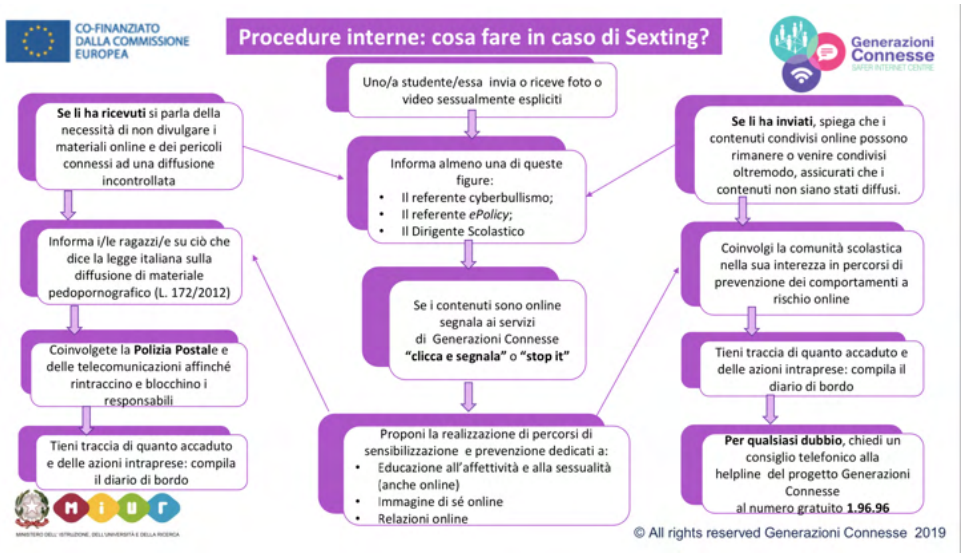
PUBBLICO TUTORE DEI MINORI
Via Longhena, 6 30175 - Marghera (VE)
041 2795925-26
pubblicotutoreminori@regione.veneto.it
http://tutoreminori.regione.veneto.it
Competenze/Servizi: segnala all'autorità giudiziaria i servizi sociali e competenti; Accoglie le segnalazioni di presunti abusi; Fornisce informazioni sulle modalità di tutela e di esercizio di questi diritti; segnala alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

5.4. - Allegati con le procedure

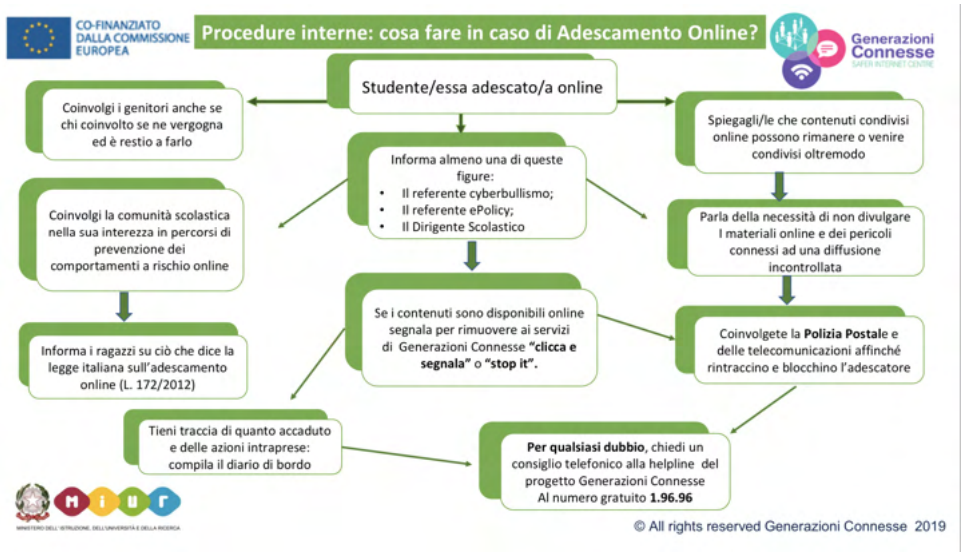
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



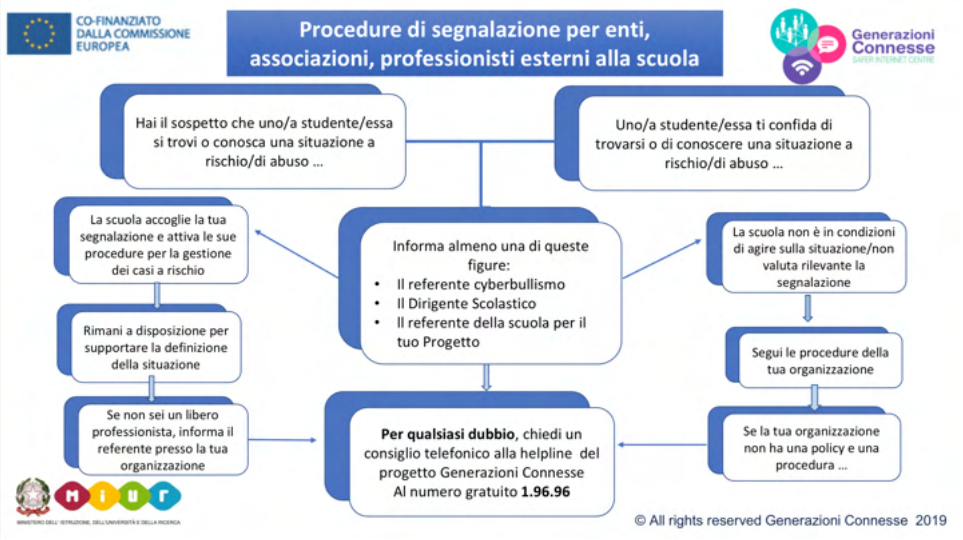
Procedure interne: cosa fare in caso di sexting?



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.