Documento di ePolicy

BGIC89300Q

ZANICA

VIA SERIO N. 1 - 24050 - ZANICA - BERGAMO (BG)

Lucia Perri

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.

Della presente E-Policy è parte integrante anche i seguenti Documenti deliberati dagli Organi Collegiali dell'Istituto:

- **REGOLAMENTO** Disciplinare per l'uso corretto dei dispositivi elettronici atto a prevenire e contrastare IL BULLISMO E IL CYBERBULLISMO;
- **LINEE GUIDA** per la promozione di comportamenti adeguati e corrette abitudini con le Tecnologie dell'Informazione e della Comunicazione (TIC);
- **PATTO EDUCATIVO DI CORRESPONSABILITA'** per un uso responsabile dei Dispositivi Digitali e per la PREVENZIONE E il CONTRASTO al BULLISMO E al CYBERBULLISMO;
- **Procedure** "Cosa fare in caso di sospetto/certo caso di bullismo/cyberbullismo"
- **Manuale delle Procedure Privacy** (MdP) inclusivo del Regolamento per l'utilizzo di Internet e della Posta Elettronica.

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.

L'Istituto nel farsi carico della formazione globale dell'individuo nella fase evolutiva individua i seguenti ruoli e responsabilità di ciascuno degli attori del percorso formativo.

Nella promozione dell'uso consapevole della rete e dei dispositivi elettronici:

1. **Dirigente Scolastico** - il ruolo del Dirigente Scolastico nel promuovere l'uso consentito delle tecnologie e della Rete include i seguenti compiti:

a. garantire che tutti/e gli/le insegnanti ricevano una **formazione** adeguata per svolgere efficacemente l'insegnamento nella didattica volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);

b. garantire che le **modalità** di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel **curriculum di studio** (promozione delle competenze digitali, educazione civica...) e nelle attività didattiche ed educative delle classi;

c. garantire la **sicurezza digitale** offline/online dei membri della Comunità Scolastica;

d. garantire l'esistenza di un sistema in grado di consentire il **monitoraggio** e il **controllo interno** della sicurezza online e offline;

e. seguire le **procedure** previste dalle norme in caso di **reclami** o attribuzione di **responsabilità** al personale scolastico in relazione a incidenti occorsi agli/lle alunni/e nell'utilizzo delle TIC a Scuola.

2. **Animatore Digitale/Team digitale** - il ruolo dell'Animatore Digitale e del Team Digitale include i seguenti compiti:

a. Progettazione di attività di formazione legate alle competenze digitali dei docenti;

b. Implementazione della tecnologia multimediale nella pratica didattica quotidiana;

c. PON progettazione e presentazione delle candidature, gestione della GPU;

d. Ricerca di materiale didattico multimediale;

e. Consulenza informatica ai docenti;

f. Supporto ai docenti in caso di attivazione della D.D.I. (Didattica Digitale Integrata)

g. Supporto organizzativo alla segreteria;

h. Informatizzazione dei registri personale dei docenti e dei documenti di valutazione degli alunni;

i. Coordinamento, supervisione e collaudo degli acquisti.

3. **Figura di sistema per la cittadinanza digitale e gestione dei processi informatici** - il ruolo di tale figura i seguenti compiti:

[Vai all'allegato n.6.1 degli Annessi]

a. Si occupa del documento E-Policy dell'Istituto;

b. E' il referente per Generazioni Connesse;

c. si occupano della diffusione della Policy fra i colleghi;

d. si relaziona con i docenti della scuola, fornendo supporto in caso di difficoltà o dubbi in merito all'attuazione della Policy;

e. diffonde la cultura dell'uso responsabile delle TIC e della Rete, anche integrando parti del curriculum della propria disciplina con approfondimenti ad hoc promuovendo, se possibile, anche l'uso delle tecnologie digitali nella didattica;

f. propone o organizza incontri formativi che hanno come tema la sicurezza on-line, i rischi della rete e la necessità di saper riconoscere situazioni potenzialmente pericolose;

g. vigilia attivamente e attentamente gli alunni quando lavorano con le nuove tecnologie e supporta docenti e alunni in caso di difficoltà;

h. Supporta il personale scolastico anche in riferimento ai rischi online;

i. Implementa l'uso (in collaborazione con la F.S. Multimendialità), nei PC scolastici, di sistemi di archiviazione (USB, memorie esterne), controlla la presenza di virus o malware.

4. **Referente Bullismo e Cyberbullismo** – il ruolo del Referente Bullismo e Cyberbullismo...

a. ha il compito di **coordinare e promuovere** le iniziative di prevenzione e contrasto del bullismo/cyber bullismo, coinvolgendo, con progetti e percorsi formativi ad hoc, studenti/essa, colleghi/e e genitori. A tal fine, può anche avvalersi della **collaborazione** delle Forze di polizia e delle associazioni e

dei centri di aggregazione giovanile del territorio;

b. può svolgere il compito di **supporto** al Dirigente Scolastico per la revisione/stesura di Regolamenti, atti e documenti (PTOF, PdM, Rav);

5. **Referente di plesso delle TIC** – il ruolo del Referente di plesso delle TIC...

6. **Team Digitale** – i compiti del Team Digitale sono quelli di dare supporto ideativo e organizzativo all'Animatore Digitale secondo il Piano d'Istituto Scuola Digitale.

7. **Direttore dei servizi generali e amministrativi** - Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti:

a. assicurare, nei limiti delle risorse finanziarie disponibili, **l'intervento di tecnici** per garantire che l'infrastruttura tecnica della Scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;

b. garantire il **funzionamento** dei diversi canali di comunicazione dell'Istituto (sportello, circolari, sito web, ecc.) all'interno delle Scuole e fra le Scuole e le famiglie degli/lle alunni/e per la notifica di documenti e informazioni del Dirigente Scolastico e dell'Animatore Digitale nell'ambito dell'utilizzo delle Tecnologie Digitali e della Rete;

c. curare la parte amministrativa legata alla elaborazione del Piano Diritto allo Studio e al Piano delle Attività attinente alle TIC.

8. Coordinatore/trice di classe/interclasse – il ruolo di queste figure include i seguenti compiti:

a. **Condividere** e gestire i "**Patti formativi**" (del Regolamento interno e il patto per un uso responsabile dei dispositivi digitali e le linee guida per una scuola libera dal cyber bullismo) con alunno/a, famiglia e Consiglio di classe/interclasse;

b. **Redigere il Regolamento** di classe in collaborazione con la classe assumendo le indicazioni della E-policy sull'uso corretto dei dispositivi digitali;

c. **Gestire** in collaborazione con il/la referente bullismo e cyberbullismo la procedura in caso di sospetto/certo

cyberbullismo.

9. **Docenti** - Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

a. **informarsi/aggiornarsi** sulle problematiche attinenti alla sicurezza nell'utilizzo delle Tecnologie Digitali e della Rete e sulla politica di sicurezza adottata dalla Scuola, rispettandone il Regolamento (si veda sezione del **sito** dell'Istituto Regolamenti);

b. garantire che le **modalità** di utilizzo corretto e sicuro delle TIC e della Rete siano integrate nel **curriculum di studio** e nelle **attività didattiche** ed educative delle classi;

c. garantire che gli/le alunni/e capiscano e seguano le **regole** per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e della Rete;

d. **assicurare** che gli/le alunni/e abbiano una chiara comprensione delle opportunità di ricerca offerte dalle Tecnologie Digitali e dalla Rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;

e. garantire che le **Comunicazioni Digitali** dei/lle docenti con alunni/e e genitori siano svolte tramite le funzionalità ***Tibitabo*** e ***Annotazioni*** del Registro Elettronico, di **Gsuite** o altre modalità stabilite dai docenti stessi nel rispetto del codice di comportamento professionale;

f. assicurare la **riservatezza** dei dati personali trattati ai sensi della normativa vigente;

g. **controllare** l'uso delle Tecnologie Digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli/lle alunni/e durante le lezioni e ogni altra attività scolastica (ove consentito);

h. nelle **lezioni** in cui è programmato l'utilizzo della Rete, **guidare** gli/le alunni/e a siti controllati e verificati, e controllare che nelle ricerche sulla Rete siano trovati e trattati solo materiali idonei;

i. **segnalare** qualsiasi problema/abuso o proposta di carattere tecnico-organizzativo al Referente delle TIC di Plesso, all'Animatore Digitale, al Team Digitale, ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella Scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;

j. **monitorare** gli/le alunni/le per riconoscerne eventuali abuso, difficoltà o disagi rilevati a Scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo attraverso l'attivazione dei protocolli;

k. **comunicare** ai **genitori** tempestivamente difficoltà, bisogni o disagi espressi dagli/le alunni/e (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;

l. **segnalare** tempestivamente al **Dirigente scolastico** e ai **genitori** qualsiasi abuso rilevato a scuola nei confronti degli/lle alunni/e in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme.

10. **Alunni/e** - il ruolo degli/lle alunni/e include i seguenti compiti:
    a. essere **responsabili**, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle Tecnologie Digitali in conformità con quanto richiesto dai docenti;
    b. avere una adeguata comprensione delle **potenzialità** offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
    c. comprendere l'importanza di adottare **buone pratiche di sicurezza online** quando si utilizzano le Tecnologie Digitali per non correre **rischi**;
    d. adottare **condotte rispettose** degli altri anche e soprattutto quando si comunica in Rete, rispettando le norme della Privacy;
    e. **esprimere** domande o difficoltà o bisogno di aiuto nell'utilizzo delle TIC o della Rete ai docenti e ai genitori.

11. **Genitori** - il ruolo dei genitori degli/lle alunni/e include i seguenti compiti:
    a. sostenere la **linea di condotta** della Scuola adottata nei confronti dell'utilizzo delle Tecnologie dell'Informazione e delle Comunicazioni nella

didattica;

b. **seguire** gli/le alunni/e nello studio a casa adottando i **suggerimenti** e le **condizioni d'uso** delle TIC indicate dai/lle docenti, in particolare controllare l'utilizzo dei Dispositivi Digitali e della Rete;

c. **relazionarsi** in modo costruttivo per concordare con i/le docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle Tecnologie Digitali o della Rete;

d. **fissare delle regole** per l'utilizzo dei Dispositivi Digitali, farne un accorto monitoraggio, tenendo di conto dell'età e tenendo sotto controllo i comportamenti che i/le figli/e hanno soprattutto nella Rete e del cellulare;

e. **accettare** e **condividere** quanto scritto **nell'e-policy** dell'Istituto.

12. Infine, gli Enti esterni e le Associazioni devono:

a. conformarsi alla politica della scuola riguardo l'uso consapevole delle TIC e della Rete;

b. promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti durante le attività che si svolgono insieme.

1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

Le **organizzazioni/associazioni** extrascolastiche e gli **esperti esterni** chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve o/e lungo periodo, dovranno prendere atto di quanto stilato nell' **E-policy** dell'Istituto e sottoscrivere un'informativa sintetica del documento in questione, presente nel contratto.

1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

1. *Condividere e comunicare la politica di e-safety agli/lle **alunni/le***

    a. **saranno informati/e** dai rispettivi docenti che la Rete e ogni Dispositivo Digitale saranno controllati e utilizzati solo dietro la loro autorizzazione;

    b. **l'istruzione** degli/lle alunni/le riguardo all'uso responsabile e sicuro della Rete precederà l'accesso alla Rete;

    c. l'elenco delle **regole** per la sicurezza online (**Regolamento aule TIC**), elaborato dal Team Digitale, sarà esposto in tutte le aule e laboratori dove si fa uso dei Dispositivi Digitali della Rete, a cura dei Referenti di Plesso delle Tic;

    d. il/la coordinatore/trice o un/a docente del Team illustrerà ad inizio anno, insieme al libretto "Scuola Sicura", illustrerà le "**PATTO EDUCATIVO DI CORRESPONSABILITA'** per un uso responsabile dei Dispositivi Digitalie per la PREVENZIONE E il CONTRASTO al BULLISMO E al CYBERBULLISMO" e il "**LINEE GUIDA** per la promozione di comportamenti adeguati e corrette abitudini con le Tecnologie dell'Informazione e della Comunicazione (TIC)" per le parti che compete loro, in cui si pone l'attenzione soprattutto sugli aspetti per i quali risultano più vulnerabili nell'utilizzo delle TIC.

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

    a. la linea di condotta della Scuola in materia di sicurezza nell'utilizzo delle Tecnologie Digitali e della Rete sarà discussa negli organi collegiali (Consigli di interclasse/intersezione, Collegio dei Docenti) e comunicata formalmente a tutto il personale con il presente documento e con i **documenti annessi**, in particolare il **Patto di Corresponsabilità** e **Linee Guida**, elaborati dal Team Digitale, sul sito web della Scuola, sul Registro Elettronico, oltre agli usuali canali di comunicazione;

b. un'adeguata **informazione/formazione** online del personale scolastico nell'uso sicuro e responsabile della Rete, sia professionalmente che personalmente, sarà fornita a tutto il personale, attraverso il sito web della Scuola, il Registro Elettronico, oltre agli usuali canali di comunicazione;

c. tutto il personale è consapevole che una condotta non in linea con il **Codice di Comportamento dei Pubblici Dipendenti** e i propri doveri professionali è sanzionabile.

3. *Condividere e comunicare la politica di E-Safety ai **genitori***

a. il documento di **E-Safety** sulla sicurezza nell'uso delle Tecnologie Digitali e della Rete, e con i documenti **annessi**, in particolare il **Patto** e **Linee Guida**, saranno disponibili ai genitori tramite Registro Elettronico e sito web della Scuola;

b. sarà incoraggiato un approccio di **collaborazione** nel perseguimento della sicurezza nell'uso delle TIC e della Rete in occasione degli incontri Scuola-famiglia, assembleari, collegiali e individuali. La relativa documentazione sarà curata dal Team Digitale;

c. l'Animatore Digitale, il Team Digitale, tutti i referenti di Plesso delle TIC e i docenti di classe forniranno ai genitori **suggerimenti** e **indicazioni** per l'uso sicuro delle Tecnologie Digitali e della Rete anche a casa, secondo le indicazioni del presente documento;

d. l'Animatore Digitale, il Team Digitale, tutti i/le referenti di Plesso delle TIC e i/le docenti di classe forniranno, anche tramite il Registro Elettronico, ai genitori, indirizzi web relativi **a risorse utili per lo studio** e a **siti** idonei ed educativi per gli/le alunni/e e i sistemi di filtraggio.

1.5 - Gestione delle infrazioni alla ePolicy

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

1. *Versante degli/le **alunni/e***

I **comportamenti disfunzionali** e/o **trasgressivi** devono essere compresi e orientati dalla comunità educante nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno/a.

Contestualmente sono previsti, oltre alle eventuali **sanzioni**, interventi di **carattere educativo** di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli/lle alunni/e 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.

Gli **interventi correttivi** previsti per gli/le alunni/e sono rapportati all'età, al livello di sviluppo dell'alunno e alla gravità dell'atto e si rimanda al "**REGOLAMENTO** per l'uso corretto dei dispositivi elettronici atto a prevenire e contrastare IL BULLISMO E IL CYBERBULLISMO".

Potenziali **infrazioni** in cui è possibile che gli/le alunni/e incorrano a Scuola o nelle attività didattiche nell'utilizzo delle Tecnologie Digitali di cui si dispone per la didattica:

a. **utilizzo** di Dispositivi Elettronici per la Comunicazione in luoghi, momenti e modalità non consentite dai Regolamenti;
b. **uso** della Rete per escludere, giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
c. registrazioni digitali che possono violare la **privacy**;
d. invio incauto o senza permesso di immagini o di altri dati personali (indirizzo di casa, telefono…);
e. comunicazione incauta e con **sconosciuti**;

f. collegamento a **siti** web, potenzialmente pericolosi, non indicati dai docenti.

Sono previsti pertanto da parte dei/lle docenti **azioni/provvedimenti "disciplinari"** quali:

a. il **richiamo** verbale;

b. il **richiamo** verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);

c. il **richiamo**, o l'**annotazione** con etichetta rossa, o **nota disciplinare** sul Registro Elettronico;

d. il **ritiro** del Dispositivo Digitale personale, secondo le **indicazioni** del Regolamento;

e. la **convocazione** dei genitori da parte degli/lle insegnanti/del coordinatore/trice;

f. la **convocazione** dei genitori da parte del Dirigente scolastico;

g. **esclusione** dalle uscite e dalle visite d'istruzione ed altre attività didattiche;

h. la **sospensione** dalle lezioni con obbligo o meno di frequenza per uno o più giorni;

i. **ammonimento** del Questore in base all'art.7 legge 71 del 2017;

j. **esclusione** dallo scrutinio finale ed eventuale allontanamento alla Comunità Scolastica;

2. *Versante del **personale scolastico***

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

a. **utilizzo** delle tecnologie e dei servizi della Scuola, d'uso comune con gli/le alunni/e, non connesso alle attività di insegnamento o al

profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;

b. **utilizzo** delle comunicazioni elettroniche con i genitori e gli/le alunni/e non compatibile con il ruolo professionale;

c. trattamento dei **dati personali**, comuni e sensibili degli/le alunni/e, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;

d. **diffusione** delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;

e. **carente** istruzione preventiva degli/lle alunni/e sull'utilizzazione corretta e responsabile delle Tecnologie Digitali e della Rete;

f. **elusione** della **vigilanza** degli/le alunni/e che può favorire un utilizzo non autorizzato delle TIC;

g. **insufficienti** interventi nelle situazioni critiche di correttivi, di contrasto o di sostegno agli/lle alunni/e, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore Digitale.

Il **Dirigente Scolastico** può:

a. **controllare** l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza;

b. **controllare** l'accesso alla Rete, la posta elettronica inviata/pervenuta a Scuola;

c. **procedere alla cancellazione** di materiali inadeguati o non autorizzati, conservandone una copia per eventuali successive verifiche.

Tutto il **personale** è tenuto a collaborare con il Dirigente Scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le **procedure** sono quelle previste dalla **legge** e dai **contratti di lavoro**.

In particolare si vedano il "**Manuale delle Procedure Privacy**" (MdP) e il "**Regolamento** per l'utilizzo di Internet e della Posta Elettronica" art. XV, elaborati dal RSPP.

3. *Versante **genitori***

In considerazione **dell'età** degli/lle alunni/le e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC a Scuola, dove gli/le alunni/e possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.

Le **situazioni familiari** meno favorevoli sono:

a. la **convinzione** che se il/la proprio/a figlio/a rimane a **casa** a usare i Dispositivi Elettronici per la Comunicazione è al sicuro e non combinerà guai;

b. una **posizione** dei Dispositivi Elettronici per la Comunicazione in una stanza o in un posto **non visibile** a tutti, quando è utilizzato dal/la proprio/a figlio/a;

c. una piena se non totale **autonomia** concessa al proprio figlio nella navigazione sul web e nell'utilizzo dei Dispositivi Elettronici per la Comunicazione soprattutto del tablet o dello smartphone;

d. un utilizzo dei Dispositivi Elettronici per la Comunicazione in **comune** con gli adulti, i quali possono conservare in memoria materiali non idonei;

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

Si rimanda al "**REGOLAMENTO** per l'uso corretto dei dispositivi elettronici atto a prevenire e contrastare IL BULLISMO E IL CYBERBULLISMO", alle "**Linee Guida**" e ai "**Patti** di Corresponsabilità".

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.

Pertanto specifici **riferimenti** alla E-policy, entro la fine dell'anno scolastico dovranno essere fatti nei seguenti documenti:

- regolamento della **Didattica Digitale Integrata**
- regolamento uso di **Gsuite**

Inoltre si ravvisa la **necessità** di **integrare,** il prima possibile, il **Regolamento di Istituto** con i seguenti **Documenti**:

- **REGOLAMENTO Disciplinare** per l'uso corretto dei dispositivi elettronici atto a prevenire e contrastare IL BULLISMO E IL CYBERBULLISMO;
- **Manuale** delle Procedure Privacy (**MdP**) e Regolamento per l'utilizzo di Internet e della Posta Elettronica, per il suo completo superamento.

Inoltre l'utilizzo **dell'Aula delle TIC**, delle postazioni e della Rete è soggetto a specifico **Regolamento**, di cui si rimanda nella sezione **Annessi**.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il ***monitoraggio*** dell'implementazione della *E-Policy* e del suo eventuale aggiornamento sarà svolta ogni anno. Tale monitoraggio verrà attivato dal Dirigente Scolastico con la collaborazione dell'Animatore Digitale, del referente del bullismo e cyberbullismo, Team Digitale, referenti di Plesso delle TIC, dal Servizio

Psicopedagogico e dagli/le docenti, tramite osservazioni e conversazioni, riunioni. Sarà finalizzato a rilevare la situazione delle classi in relazione all'uso sicuro e responsabile delle Tecnologie Digitali e della Rete.

L'aggiornamento della **E-Policy** sarà curato dal Dirigente scolastico, dall'Animatore Digitale, dal Team Digitale, dagli Organi Collegiali, e da ogni altra articolazione istituzionale a seconda degli aspetti considerati. **L'editing** del documento sarà curato dalla figura specifica incaricata.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti.
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori.

Azioni da svolgere nei prossimi 3 anni:

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

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.

Nell'a.s. 2018/19 il Team Digitale ha elaborato, anche in riferimento a precedenti 'Piani di Sviluppo delle TIC' costruiti negli anni, un **Piano Digitale di Scuola**, approvato dal Collegio dei Docenti, con gli obiettivi di migliorare le competenze di Cittadinanza relative alle TIC versante alunni/e, di mettere in condizione i docenti di promuovere tali competenze in modo sicuro, professionale e consapevole.

In particolare il Team digitale ha elaborato, ripartendo dal documento scritto nell'a.s.2012/13 e dalle attività di aggiornamento sui Curricoli, due testi che sia sintesi delle parti presenti nelle Indicazioni Nazionali relativo alle TIC nei Curricoli, punto di **sviluppo** per un **Curricolo Digitale d'Istituto,** in cui sono stati individuali gli obiettivi di apprendimento che ogni disciplina deve perseguire e le dimensioni ed indicatori per individuare i livelli di padronanza.

Quest'anno la **valutazione** della competenza digitale sarà anche per le classi 1° e 2° della scuola secondaria, completando la relativa **tabella** dei descrittori.

I documenti elaborati sono:

- **Curricolo** sulle **competenze digitali** per gli/le **studenti/e:** i traguardi attraverso gli obiettivi di apprendimento delle singole discipline
- **Rubriche** generali per il curricolo di istituto per competenze: la **competenza digitale**

La **pandemia** ha imposto la chiusura delle scuole l'anno scorso per un quadrimestre intero e questo anno diverse classi, per varie ragioni, si sono trovate a fare Didattica a Distanza (**DAD**) o Didattica Digitale Integrata (**DDI**). Questo ha comportato che molti/e alunni/e hanno acquisito dimestichezza con le TIC ed in particolar modo con la piattaforma **Gsuite**. Aspetto molto positivo è che si sono rilevati pochi **comportamenti disfunzionali** all'uso corretto dei dispositivi digitali.

Più problematica è stata l'attivazione della DAD per le **classi precedenti** alla secondaria di I grado, per limiti di **varia natura interni all'Istituto** e in parte per l'inadeguatezza dei dispositivi digitali e relativo collegamento accettabile.

All'interno **dell'offerta formativa** nel corso del corrente anno scolastico, sono stati previsti alcuni **eventi** volti alla promozione alla **Cittadinanza Digitale** attiva per educare gli/le alunni/le al rispetto delle regole nei comportamenti con le Tecnologie Digitali:

- su bisogno interventi nell'ambito del progetto psicopedagogico su tematiche legati **all'educazione dell'affettività** problemi quali il sexting, l'adescamento ecc.;
- Progetto **settimana della gentilezza** – **Nodo blu** – **Parole non ostili**: la buona comunicazione contro hate specch, il cyberbullismo... per il rispetto dell'altro/a;
- **Robotica** in classe: il coding;
- **Liberi in rete**: progetto incentrato sui nuovi modi di comunicare e di essere in relazione e buone prassi per la prevenzione dei comportamenti a rischio online e offline [legge 71 del 2017].

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.

Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica, non esauribile nell'arco di un anno scolastico, prevede momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'istituto, con la condivisione delle conoscenze dei singoli.

Si è concluso l'anno scorso il progetto **ATS-Cremit**, sulle Buone Prassi nell'Uso delle TIC" e due anni fa l'aggiornamento per costruzione di un curricolo d'istituto in cui si è messo le basi per lo **sviluppo** anche della **competenza digitale**.

Purtroppo diverse attività sono state bloccate in conseguenza della **chiusura** delle scuole e delle restrizioni imposte.

Sono previsti **momenti** di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'Istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale/Team previsto dal PNSD e corsi di aggiornamento online, anche attraverso la fruizione dei materiali messi a disposizione dall'Animatore digitale stesso con la creazione di bacheche virtuali sul sito della scuola (manuali, guide e tutorial per la didattica con le TIC).

Particolare attenzione è data alla **conoscenza** delle funzioni del **Registro elettronico** e della piattaforma **GSuite**, vincolando gli/le insegnanti a far riferimento solo a questa e non affidandosi ad altre improprie e personali soluzioni.

2.3 - Formazione dei docenti

sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

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

L'Istituto Comprensivo si avvale della **figura** dell'Animatore digitale che, con il Dirigente Scolastico e il D.S.G.A., collabora per raggiungere gli obiettivi di innovazione del PNSD nella scuola. Inoltre, a partire dall'anno scolastico 2017-2018 è attiva la **figura** del Referente d'Istituto per le attività di prevenzione e contrasto al bullismo e al cyberbullismo (L.107/2015). La formazione sull'utilizzo consapevole e sicuro delle TIC è stata estesa ad altre figure, in funzione della costituzione di un Team Digitale.

Si rende, comunque, necessaria la **formazione** di tutti i **docenti** sull'uso consapevole e sicuro di Internet e sui rischi della rete. Infatti il percorso di formazione specifica dei docenti non può essere esaustivo, ma deve essere **permanente** in relazione all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono in maniera costante ed autonoma i/le ragazzi/e. Pertanto si rende necessario che si prevedeano momenti di **autoaggiornamento** e di **formazione** personale o collettiva, senza escludere la formazione attraverso corsi interni o esterni, mediante seminari, conferenze e dibattiti, oppure con **formazione a distanza** o con la partecipazione ad **iniziative al di fuori** della programmazione d'Istituto.

Quindi il percorso della **formazione** specifica dei **docenti** sull'utilizzo consapevole e sicuro della Rete, ha previsto e prevederà momenti di informativi-formativi nell'ambito delle 40 ore collegiali, momenti di formazione personale o collettiva di carattere **permanente**, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

Il Team Digitale a giugno/settembre di ogni anno scolastico elabora una serie di proposte sulle TIC da inserire nel **Piano di Aggiornamento** dell'Istituto in coerenza con le azioni del **Piano d'Istituto Scuola Digitale** .

Nell'anno l'a.s. **2019/20** sono stati realizzati incontri serali genitori/docenti sulla sicurezza nel web, per il progetto "**Liberi nella Rete**", aperto a genitori/alunni/docenti e un corso per la gestione della piattaforma **GSUITE**.

Anche per l'a.s.**2020/21** verranno **riproposte** le stesse attività di formazione e si proporrà l'adesione da parte dei docenti ai corsi di formazione del progetto **Safer Internet Centre** – **Generazioni Connesse**.

Saranno predisposti **link** e **pagine** online per la messa a disposizione e la condivisione di materiali per **l'aggiornamento** sull'utilizzo consapevole e sicuro della Rete, collegata alla homepage del sito scolastico [www.iczanica.edu.it]. Qui è possibile trovare materiali informativi sulla sicurezza nella Rete per l'approfondimento personale, per le attività con gli/le alunni/e e gli incontri con i genitori, costituiti da guide in pdf, video, manuali a fumetti, link a siti specializzati e contributi della Polizia di Stato, dell'Arma dei Carabinieri, di Telefono Azzurro, dal sito "Generazioni connesse", ecc..

La stessa operazione di **diffusione** di **materiali**, utili alla sicurezza in Rete e nella gestione dei Dispositivi Digitali per la comunicazione, sarà tramite il Registro Elettronico.

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.

Scuola e famiglia quindi sono chiamate a collaborare per garantire la crescita formativa di ciascun alunno, perciò **stipulano,** ad integrazione della **E-safety Policy** e del **Regolamento disciplinare**, all'inizio dell'anno scolastico, e a cui sono tenuti ad adeguarsi, il **PATTO EDUCATIVO DI CORRESPONSABILITA'** per un uso responsabile dei Dispositivi Digitali e per la PREVENZIONE E il CONTRASTO al BULLISMO E al CYBERBULLISMO, presentato durante le lezioni dei rappresentanti dei genitori ad ottobre e gli open-day nel mese di dicembre.

La Scuola si impegna, attraverso comunicazioni nel Registro Elettronico, nelle riunioni degli Organi Collegiali e nel sito della Scuola [https://www.iczanica.edu.it], alla diffusione delle **informazioni** e delle **procedure** contenute nel documento (**E-Safety Policy**) per portare a conoscenza delle famiglie il "**REGOLAMENTO Disciplinare** per l'uso corretto dei dispositivi elettronici atto a prevenire e contrastare IL BULLISMO E IL CYBERBULLISMO " e prevenire i rischi legati a un utilizzo non corretto della Rete.

L' Istituto, per cui, ha attivato **iniziative** per sensibilizzare le famiglie all'uso consapevole delle TIC e della Rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono stati previsti incontri per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine.

In particolare, nell'a.s. **2017/18** sono stati organizzati 4 incontri dal titolo "**Stare in Rete**, comunicare con la Rete: tra opportunità e rischi" in cui si è riflettuto sulle regole e le leggi, sugli aspetti psicologici e si è fatto il punto su chi è il Referente bullismo e cyberbullismo, il protocollo denuncia di atti, sulla privacy violata, sui moduli di segnalazione tramite il sito dell'Istituto Comprensivo; si sono presentati dati di un questionario distribuito agli/e alunni/e su bullismo e cyberbullismo dalla 5° primaria alla 3° secondaria. Ed infine un'attività operativa con i genitori dotati di Dispositivi Digitali per la comunicazione a cura dei docenti del Team Digitale dell'IC di Zanica in cui si è fatta l'analisi dei principali social e azioni su come gestire la privacy e su come fare richieste per la rimozione dei contenuti inappropriati.

Lo stesso percorso formativo è stato riproposto anche per l'a.s.**2018/19** e lo è stato per l'a.s. **2019/20**, con il progetto "**Liberi in Rete**" in collaborazione con i Comitato Genitori dei due comuni di Comun Nuovo e Zanica.

Quindi saranno favoriti momenti di confronto e discussione, anche sulle **dinamiche** che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare

riferimento alla prevenzione del cyberbullismo, da farsi anche nelle ore dei colloqui tra docenti-genitori.

Sul **sito scolastico** e sulla relativa bacheca virtuale relativa a "**Generazioni connesse**" sono stati messi in condivisione materiali dedicati ad alunni e alle famiglie come guide in formato .pdf e video che possono fornire spunti di approfondimento e confronto.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni

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

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

Il **personale scolastico** è "incaricato del trattamento" dei dati personali (degli/lle alunni/e, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi. Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli/lle alunni/e eccedenti i trattamenti istituzionali obbligatori tramite apposito modulo.

In merito alla **protezione dei dati personali**, si fa riferimento a quanto previsto dal Decreto Legislativo del 30 giugno 2003, n.196 (cosiddetto Codice della Privacy), integrato dal D. Lgs. 10 agosto 2018, n. 101, e dal GDPR (General Data Protection Regulation) n. 679 del 2016.

All'atto dell'iscrizione viene fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, come per l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine e/o il nome del proprio figlio/a all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola. A tale proposito si evidenzia che le immagini e le riprese audio-video realizzate dalla scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della scuola tramite il sito Internet di Istituto. L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la propria dignità personale ed il decoro e comunque per uso e/o fini diversi da quelli sopra indicati. Inoltre, in caso di partecipazioni a concorsi o manifestazioni l'Istituto richiede apposita autorizzazione, chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato all'interno di modulistica o sul proprio sito web istituzionale. La formula utilizzata per chiedere il consenso è, in ogni caso, comprensibile, semplice e chiara. Pertanto, in ottemperanza al GDPR (General Data Protection Regulation) e al D. Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre, la scuola non si impegna solo a tutelare la privacy degli/lle studenti/esse e delle loro famiglie, ma anche ad informare e soprattutto rendere

consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

- Si veda il **sito** del **Miur**: https://www.miur.gov.it/privacy-tra-i-banchi-di-scuola

e quello del **Garante della Privacy**: https://www.garanteprivacy.it/scuola

---

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.

L'accesso a Internet è possibile e consentito per la **didattica** in tutti i plessi attraverso reti WiFi o via cavo. La Dirigenza e l'Amministrazione hanno una **rete separata**. Le impostazioni dei computer presenti nei laboratori e nelle aule sono definite e manutenute dal/la responsabile delle TIC di scuola, il/la quale segnala alla segreteria eventuali malfunzionamenti e disservizi. L'accesso a Internet, attraverso i dispositivi della scuola da parte degli/lle studenti/esse, avviene solo in presenza dell'insegnante, il quale è responsabile del comportamento degli/lle alunni/e, delle macchine e del software che utilizzano. È possibile effettuare installazioni e aggiornamenti di software dopo avere avuto l'autorizzazione dal/la referente delle TIC di scuola o dal Dirigente o dall'Animatore Digitale.

In quasi tutti computer a disposizione del personale scolastico non amministrativo sono installati **due account**, un amministratore al quale è permesso di effettuare modifiche sostanziali o installare e disinstallare programmi e un utente limitato senza password, protetti da firewall ed antivirus aggiornati dai Referenti di Plesso delle TIC.

I docenti possono accedere alla propria sezione del **registro elettronico** con credenziali personali.

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.

Per **l'accesso al sistema informatico per la didattica**, nei laboratori multimediali i/le docenti prenotano il proprio accesso, scrivendo su un registro la data e l'orario di utilizzo del laboratorio. Per i/le docenti che devono disbrigare atti burocratici e di documentazione delle loro attività professionali devono fare uso delle postazioni situate nelle sale

dedicate a loro stessi. I/le docenti sono invitati, se non indicato contrariamente volta per volta, a salvare i file sui supporti rimovibili personali. Le postazioni del laboratorio funzionano preferibilmente come stazioni di lavoro e non come archivi.

L'accesso al sistema informatico per la didattica (aule TIC, classi, aule specializzate) è consentito al personale al momento senza l'assegnazione di una password.

I **tablet della scuola e i pc** nelle **aule docenti** è opportuno che abbiano un accesso tramite password, su cui non si deve salvare nessun dato sensibile.

L'accesso ai portali istituzionali come SIDI, Istanze on-line, alla Segreteria Digitale, PON ecc. prevede l'uso di credenziali personali.

Le **chiavette personali**, devono avere un software che permette l'accesso con **password**. Lo stesso dicasi per ogni altro dispositivo digitale personale, usato per l'archiviazione di informazioni rilevanti a scuola devono avere attivo lo schermo di blocco attivabile con password.

Si ricorda che in caso di **perdita** o **furto** di un dispositivo digitale e/o memoria removibile, con dati sensibili, se ne deve dare comunicazione alla Dirigente e al Garante della Privacy.

E-mail.

Gli **account di posta elettronica** sono solo quelli istituzionali utilizzati ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam.

Dall'a.s. **2019/20** tutti gli/le alunni/le, i docenti e il personale di segreteria hanno un loro **account**. I/le docenti gestiscono le attività collaborative didattiche tramite la piattaforma **GSUITE** ed ogni docente dovrà attenersi a questa regola. Le **deroghe** devono essere richieste alla Dirigente.

Sito web dell'Istituto

La Scuola ha un **sito web** [www.iczanica.edu.it]. Tutti i contenuti, compreso quelli del settore didattico, sono pubblicati **Webmaster**, esterno all'Istituto, che ne valuta su mandato del Dirigente Scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc..

L'Istituto Comprensivo di Zanica detiene i **diritti d'autore** di tutte le

informazioni che sul sito sono pubblicate sotto **Licenza non commerciale libera**

(https://creativecommons.org/licenses/by-nc-sa/4.0/deed.it). *Social network.*

Attualmente l'Istituzione Scolastica non ha creato una pagina Social col proprio profilo o ha autorizzato il personale scolastico a utilizzarli per nome e per conto della stessa, ne da diffida a che ciò possa verificarsi senza l'espressa autorizzazione del Dirigente.

Tuttavia si riconosce la prassi da parte dei **genitori** e dei **docenti** di partecipare consapevolmente ai Social Network per le comunicazioni funzionali all'organizzazione e all'andamento scolastico seguendo criteri di efficacia, di pertinenza, di rispetto dei ruoli, di correttezza, anche della Privacy, secondo uno spirito di collaborazione e di effettiva risoluzioni di problemi che possono nascere nel corso dell'anno scolastico, evitando di esprimere giudizi inappropriati sull'operato degli/lle altri/e alunni/e o del personale scolastico o dei genitori, giudizi che una volta pubblicati nel social, comportano sempre un'assunzione di responsabilità amministrativa e/o penale di chi li ha scritti o a che semplicemente diffusi.

Pertanto si suggerisce di adottare delle regole per una comunicazione efficace e pertinente, che stabiliscano le modalità su chi amministra, su come e cosa si comunica... ecc..

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.

1. Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc..

E' consentito per ragioni esclusivamente didattiche e sotto la supervisione del docente **l'uso di Dispositivo Digitale** e/o per la comunicazione, favorendo comportamenti responsabili dei Dispositivi personali con attività didattiche anche con la metodologia del **BYOD**. Per la dimensione personale e in caso di urgenza è disponibile il telefono fisso della Scuola per le comunicazioni tra gli/le alunni/e e le famiglie, su autorizzazione e con il controllo dell'identità dell'interlocutore che deve essere verificata dal personale della Scuola.

2. Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc..

E' consentito l'uso dei Dispositivi Digitali personali a scopo didattico ed integrativo di quelli scolastici disponibili. Negli altri momenti di presenza a Scuola è consentito l'utilizzo dei Dispositivi Digitali per la comunicazione **solo** per comunicazioni personali di carattere urgente ed è permesso l'uso degli stessi per comunicazioni relative alle attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

Si **sconsiglia** le comunicazioni Scuola-famiglia tramite Dispositivi Digitali personali, come il far parte a gruppi Social con genitori e ancor meno con alunni/e. Si dia la preferenza ai canali istituzionali della Scuola, tra cui la funzionalità **Tibidabo** del Registro Elettronico o la posta della **piattaforma Gsuite**.

3. Per il personale della Scuola: gestione degli strumenti personali - cellulari, tablet ecc..

Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo dei Dispositivi Digitali personali e non, **solo** per comunicazioni personali di carattere urgente o per attività funzionali al proprio ruolo professionale.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

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

Scegliere almeno 1 di queste azioni:

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

1. Rischi

I **rischi** effettivi che si possono correre a **Scuola**, ma soprattutto **al di fuori** e il cui effetto può avere ricadute negative sul rendimento scolastico e non solo, nell'utilizzo delle TIC da parte degli/lle alunni/e,

derivano da un uso non corretto del telefono cellulare personale o di accessi impropri a siti pericolosi tramite Personal Computer della Scuola collegati alla Rete.

Eludendo la sorveglianza degli insegnanti e/o dei genitori, soprattutto attraverso i telefoni cellulari o gli smartphone, dotati di particolari applicazioni e di collegamento a internet, potrebbero:

a. parlare e scrivere messaggi con i genitori in momenti e con modalità non consentite;
b. riprendere, scaricare e spedire foto personali o intime, proprie o di altri, video con contenuti indecenti o violenti;
c. accedere a internet e a siti non adatti ai minori;
d. ascoltare musica e giocare con i videogiochi non consigliati ai minori;
e. leggere la posta elettronica e comunicare o chattare con sconosciuti;
f. inviare o ricevere messaggi molesti e/o minacciosi;
g. in relazione ai punti sopra esposti essere causa o vittima di cyberbullismo.

2. Azioni

Le **azioni** previste di **prevenzione** nell'utilizzo delle TIC sono le seguenti:

1. Informare e formare i docenti, il personale ATA e gli/le allievi/e sui rischi che un uso non sicuro delle Nuove Tecnologie della Comunicazione può favorire, con modalità proposte dal Team Digitale in collaborazione con il Servizio Psicopedagogico ed altre articolazioni, e condivise con il personale della Scuola attraverso gli Organi preposti a inizio e fine anno scolastico;
2. Impegnare i genitori alla firma consapevole e al rispetto dei "**Patti di Corresponsabilità**";
3. Richiedere ai genitori che si impegnino altresì ad essere partecipi ed attivi nel seguire il percorso del proprio/a figlio/a in particolare nelle attività di formazione legate ad un uso corretto delle Nuove Tecnologie Digitali;
4. Fornire ai genitori, ad inizio anno, informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli/lle alunni/e

eccedenti i trattamenti istituzionali obbligatori (si veda la **Liberatoria** per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio/a figlio/a, negli **Annessi**);

5. ad inizio anno, nella elaborazione del "**Regolamento di Classe"** con gli/le alunni/e, far prendere visione delle norme che richiedono il rispetto delle regole per un uso corretto delle TIC come da "**Regolamento di Istituto"**. In particolare:
    i. che non è consentito l'utilizzo dei Dispositivi Digitali per la comunicazione personale degli/lle alunni/e a Scuola, in quanto per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della Scuola, supervisionato dal personale addetto al centralino, che prima di passare la telefonata si accerta dell'identità dell'interlocutore;

    ii. che è consentito l'utilizzo personale del cellulare/smartfone solo in casi particolari ed eccezionali, e comunque sotto la supervisione dell'insegnante, che eventualmente si accerta preventivamente dell'identità dell'interlocutore;

Le azioni di **contenimento** degli **incidenti** previste sono le seguenti, previa convocazione dei **Genitori**:

a. se la **condotta incauta** dell'/a alunno/a consiste nel fare circolare immagini imbarazzanti, di natura sessuale, sulla Rete, è necessario fare una rapida valutazione se ciò possa costituire reato o meno (si veda punto e) ed eventualmente farle rimuovere: invitare i genitori a contattare il Service Provider e se il materiale postato viola i termini e le condizioni d'uso del sito far richiedere la loro immediata rimozione;

b. se l'alunno/a viene **infastidito** od **offeso**, suggerire di modificare i dettagli del proprio profilo sistemandolo su "privato", in modo tale che solo gli utenti autorizzati siano in grado di vederlo (MSN messengers, siti social network, Skype etc.), o suggerire di bloccare o ignorare particolari mittenti, di cancellare il loro nominativo dalla lista degli amici con i quali regolarmente chatta, di inserire il compagno o la persona che offende, per quanto riguarda l'e-mail, tra gli indesiderati. Se esiste, togliere l'opzione "amici degli amici" e similare;

c. **consigliare** di cambiare il proprio indirizzo e-mail, contattando

l'e-mail provider, di scaricare un'applicazione che blocchi chiamate e messaggi da numeri indesiderati o, se necessario, cambiare il numero telefonico provato contattando l'operatore telefonico;

d. in caso di materiale offensivo, valutare se conservare una copia di detto materiale se necessario per ulteriori indagini, e tramite i genitori, chiedere agli/lle allievi/e di indicare a chi e dove lo hanno spedito;

e. Se si dubita che il materiale digitale abbia dei profili di illegalità chiedere immediata consulenza al Referente Bullismo e/o al Dirigente. In situazioni particolari si può telefonare al **114**, oppure al numero verde **800 66 96 96** attivo dal lunedì al venerdì, dalle 10 alle 13 e dalle 14 alle 19, oppure contattare le Forze di Polizia.
In caso di foto e video pedopornografici, si deve confiscare il telefonino o altri dispositivi ed evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto, poiché ciò è reato per chiunque e chiedere immediata consulenza al Referente Bullismo e/o al Dirigente oppure telefonare al **114**, oppure al numero verde **800 66 96 96** attivo dal lunedì al venerdì, dalle 10 alle 13 e dalle 14 alle 19, oppure contattare le **Forze di Polizia**.

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).

I comportamenti definibili di "Bullismo/Cyberbullismo" possono esprimersi nelle forme più varie e non sono tratteggiabili a priori; se non contestualizzandoli. Le caratteristiche che aiutano a individuarli e a distinguerli dallo scherzo, dalle intemperanze caratteriali, dai diverbi usuali fra i ragazzi sono la costanza nel tempo e la ripetitività, l' asimmetria (disuguaglianza di forza e di potere), il disagio provocato nella/e vittima/e.
Il Bullismo/Cyberbullismo si esplica infatti con comportamenti e atteggiamenti costanti e ripetitivi di arroganza, prepotenza, prevaricazione, disprezzo, dileggio, emarginazione, esclusione ai danni di una o più persone, agiti da un solo soggetto, ma in genere da un gruppo.
Nel caso particolare del Cyberbullismo le molestie sono attuate attraverso strumenti tecnologici:

a. invio di sms,messaggi in chat, e-mail offensive o di minaccia;
b. diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o email nelle mailing-list o nelle chat-line;
c. creazione di gruppi contro, falsi profili con epiteti offensivi, con foto, video della vittima;
d. pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata.

Il Bullismo/Cyberbullismo in particolare può originarsi anche dall'esasperazione di conflitti presenti nel contesto scolastico. Il

conflitto, presente in ogni normale intenzione, è da considerarsi come un campanello d'allarme e può degenerare in forme patologiche quando non lo si riconosce e gestisce in un'ottica evolutiva dei rapporti, di negoziazione e risoluzione. Se non gestito positivamente, infatti, il conflitto rischia di mutarsi e provocare effetti distruttivi sulle relazioni (prevaricazione e sofferenza) e sull'ambiente (alterazione del clima del gruppo-classe).
In considerazione dell'età degli/lle alunni/e possono prefigurarsi alcune forme di interazioni che possono evolvere verso tale fenomeno. Per prevenire e affrontare il Bullismo/Cyberbullismo dunque i/le docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, anche mediante interventi del Servizio Psicopedagogico, coinvolgendo i genitori degli/lle allievi/e. L'elemento fondamentale per una buona riuscita dell'intervento educativo è infatti la corretta, compiuta e convinta ristrutturazione dell'ambiente sociale in cui tale fenomeno si verifica, e in particolare delle relazioni nel contesto della classe. Gli atteggiamenti degli/lle alunni/e, così come quelli dei loro genitori, possono giocare un molto significativo nel ridurre la dimensione del fenomeno.
Gli **interventi mirati sul gruppo classe** possono sono gestiti direttamente dalle/i docenti oppure dal Servizio Psicopedagogico in collaborazione con gli/le docenti e d'intesa con le famiglie - ad esempio con percorsi di mediazione volta alla gestione positiva del conflitto, con gruppi di discussione (circle time), con rappresentazioni e attività di role-playng sull'argomento del Bullismo/Cyberbullismo, con simulazione di casi da affrontare con strategie del problem solving.
Devono essere intrapresi anche **percorsi individualizzati di sostegno alle vittime**, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i **prevaricatori** essere destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali.
In relazione alle manifestazioni socio-affettive fra pari, al linguaggio sessualizzato o "volgare", al fine di evitare prevaricazioni e imbarazzo o disagio, i docenti intervengono:

a. per favorire negli/lle alunni/e un buon rapporto con il proprio corpo e per far percepire meglio eventuali violazioni dei limiti di prossimità o di "confidenza" ed imparare ad opporvisi;
b. per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito e determinazione nel rifiutare i contatti anche "a distanza" sgradevoli o "strani";
c. per rendere consapevoli gli/le alunni/e del diritto al rispetto dei propri limiti e di quelli altrui;
d. per far capire ai/lle ragazzi/e che l'interazione on-line deve sottostare a delle regole di buon comportamento, né più né meno

della comunicazione a viso aperto, quale quella della vita reale.

Inoltre la Scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia altresì di servirsi dello sportello di ascolto del Servizio Psicopedagogico.
Promuove e supporta la richiesta delle famiglie rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi comunali e alla ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).

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.

Si potrebbe, quindi, pensare ad attività di analisi e produzione mediale.

4.4 - Dipendenza da Internet e gioco online

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

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

La scuola ha la possibilità di fare formazione e di indicare strategie per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia.
Gli elementi che contribuiscono al benessere digitale sono:

- la ricerca di equilibrio nelle relazioni anche online;
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali;
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile;
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

Questo è un argomento trasversale, se ne può parlare quando si parla di cittadinanza digitale, di cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete; tanto più può essere utile dedicare al tema un momento specifico e riflettere con studenti e studentesse per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.
La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.
Si potrebbe riflettere insieme su: come trascorri il tempo on line? Quando aggiunge valore alla tua vita e quando ti fa perdere tempo? Quale atteggiamento potrei cambiare quando sono online? Che ruolo ha e deve avere la tecnologia (internet o il gioco) nella mia vita?
Allo stesso modo quando parliamo di videogiochi, dobbiamo pensarli non in termini negativi ma di benessere digitale. Sono parte del mondo di studenti e studentesse. E, allora, riflettiamo insieme a ragazzi e

ragazze su: quando sono una risorsa? Accedono a contenuti adeguati all'età? A che ora e per quanto tempo li usano? Diventa utile riflettere con i ragazzi e le ragazze rispetto all'uso della tecnologia in termini di qualità e tempo.
Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi.
Strutturare regole condivise e stipulare con loro una sorta di "patto" d'aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula (Es. adoperando la LIM o il dispositivo personale. Si veda il BYOD di cui abbiamo parlato nel precedente modulo). È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/lle studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.

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.

Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile, perché facilmente modificabili, scaricabili e condivisibili, e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che riguardano minorenni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico.

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn", letteralmente "vendetta porno", fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

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.

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove.
Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video...).
L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.
I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi, ma anche di provare un senso di colpa per essere caduti in trappola ed essersi fidati di uno sconosciuto.
Inutile sottolineare che nei casi più estremi in cui l'adescamento porta

ad un incontro fisico e ad un abuso sessuale un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.
Per **consigli** e per un **supporto** è possibile rivolgersi alla **Helpline** di Generazioni Connesse (**19696**): operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

4.7 - Pedopornografia

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

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

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

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

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

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

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

Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto e primariamente, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario.

Parallelamente, per salvaguardare il benessere psicofisico degli alunni coinvolti nella visione di questi contenuti, sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.

Se si è a conoscenza di tale tipologia di **reato** è possibile far riferimento alla: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato online.

Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità. L'abuso sessuale online rappresenta una particolare declinazione dell'abuso sessuale su bambini/e, ragazzi/e, la

cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale online si manifesta producono effetti sulle vittime che si aggiungono e moltiplicano a quelli associati all'abuso sessuale.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

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

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

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

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

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

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

Scegliere almeno 1 di queste azioni:

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

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

☐ Promuovere incontri e laboratori per studenti e studentesse dedicati all'

Educazione Civica Digitale.

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online**: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona 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.

Gli/le alunni/e possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni/e o di altri/e e riferire spontaneamente o su richiesta l'accaduto ai/lle docenti. I fatti riferiti possono essere accaduti **anche al di fuori della Scuola**. Anche confrontandosi periodicamente con gli/le alunni/e sui rischi delle comunicazioni on-line, i minori possono riferire di fatti o eventi personali o altrui che "allertano" l'insegnante. La"prova" di quanto riferito può essere presente nella memoria degli Strumenti Tecnologici utilizzati, può essere mostrata spontaneamente dall'alunno/a, può essere presentata da un reclamo dei genitori, può essere notata dall'insegnante che si accorge dell'infrazione in corso.
Mentre il/la docente è autorizzato/a a controllare le strumentazioni della Scuola, per **controllare** l'uso degli strumenti tecnologici di un/a alunno/a si deve rivolgere al genitore o al Tutore.
I contenuti "pericolosi" comunicati/ricevuti a/da altri, messi/scaricati in Rete, ovvero le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli Strumenti Digitali utilizzabili anche a Scuola attualmente dai minori (ad es. cellulare/smartphone/tablet /pc personale e il pc collegato a internet della Scuola) per gli/le alunni/e possono essere i seguenti:

a. Contenuti afferenti alla **privacy** (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici/he, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
b. 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.);
c. 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.

Si danno alcune indicazioni particolari.
Per il **cellulare/ smartphone** ci si può assicurare che l'alunno/a vittima salvi sul suo Dispositivo ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.

Gli/le insegnanti, anche con l'ausilio tecnico dell'Animatore Digitale e/o del Collaboratore Tecnico delle TIC, possono provvedere ugualmente a conservare le prove della condotta incauta, scorretta o dell'abuso rilevate sui Dispositivi Digitali della Scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto. Qualora ci si dovesse accorgere che l'alunno, usando il Computer della scuola, si sta servendo di un servizio di messaggeria istantanea, programma che permette di chattare in linea tramite testo, l'insegnante può copiare, incollare e stampare la conversazione. Per gli eventuali collegamenti non autorizzati a siti social network, video-hosting sites e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su un Elaboratore testi. Per le e-mail si può stampare la mail o conservare l'intero messaggio, compresa l'intestazione del mittente.

Conservare la **prova** è utile per far conoscere l'accaduto in base alla gravità ai genitori degli/lle alunni/e, al Dirigente Scolastico e per le condotte criminose agli Organi Competenti. Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno/a, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque da essere comunicate ai genitori e per fatti rilevanti anche al Dirigente scolastico; per quelle criminose, si dovrà fare riferimento, tramite Dirigente o Docente Delegato agli Organi Competenti. In particolare la segnalazione viene fatta ad entrambe le famiglie, se oltre alla vittima, anche l'autore della condotta negativa è un/a altro/a alunno/a.
Per le segnalazioni di fatti rilevati sono previsti le seguenti **modalità** che i docenti possono utilizzare sulla base della gravità dell'accaduto:

a. Un Richiamo comportamentale o una Annotazione sul Registro Elettronico;
b. Convocazione scritta/telefonica e colloquio (utilizzare lo strumento Annotazione con icona gialla del Registro Elettronico) con i genitori degli/lle alunni/e, da parte dei/lle docenti;
c. Relazione scritta al Dirigente scolastico, anche tramite la Referente del Bullismo.

In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie più brevi.
Per i **reati** meno gravi, la legge rimette ai genitori degli/lle alunni/e la scelta di richiedere il sanzionamento del colpevole, attraverso la querela.

Per i **reati** più gravi, come la pedopornografia gli operatori scolastici hanno l'obbligo di effettuare la denuncia, tramite il Dirigente Scolastico, all'autorità giudiziaria o più semplicemente agli Organi di Polizia territorialmente competenti.
In particolare per i fatti criminosi, ai fini della denuncia, la relazione deve essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

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

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

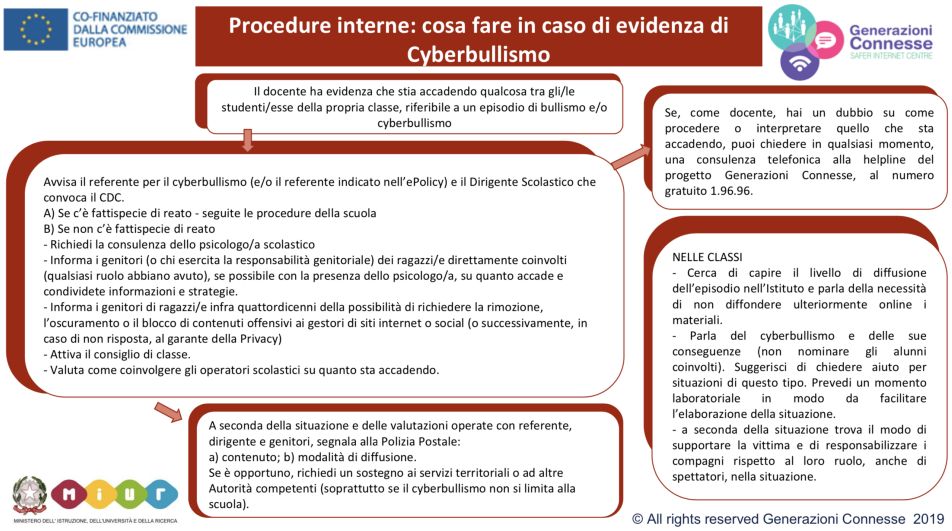
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello

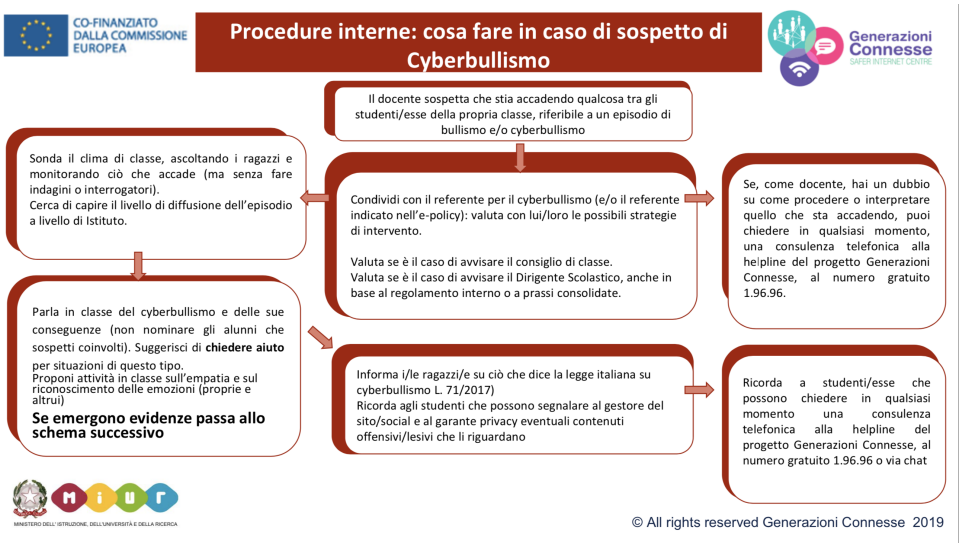
psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

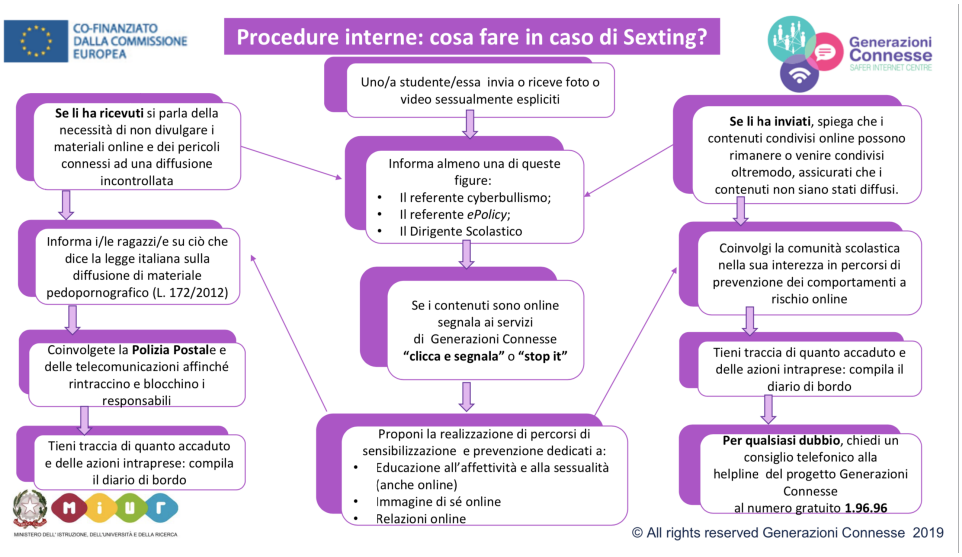
5.4. - Allegati con le procedure

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

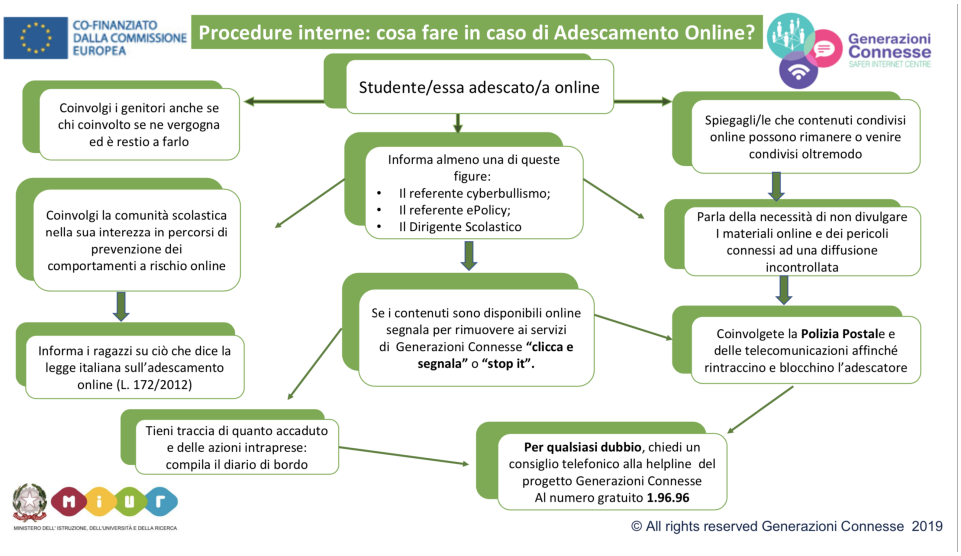




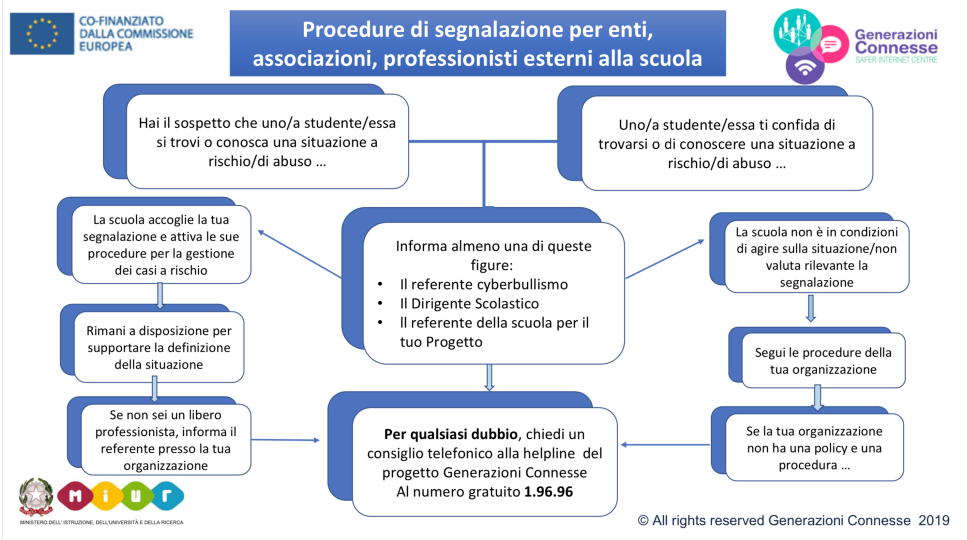
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

Non è prevista nessuna azione.