Documento di ePolicy

CHIC83000G

I.C. FARA FILIORUM PETRI

VIA SAN NICOLA 2 - 66010 - FARA FILIORUM PETRI - CHIETI (CH)

Ivana Marroncelli

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

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

Perché è importante dotarsi di una E-policy?

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

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

Il presente documento vuole descrivere la linea di condotta dell'Istituto Comprensivo di Fara Filiorum Petri" nei confronti dell'utilizzo delle nuove tecnologie nella didattica.
In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni

delle tecnologie digitali e di internet, di far acquisire loro corrette norme comportamentali nonché procedure e competenze “tecniche” per prevenire e fronteggiare le problematiche che derivano da un utilizzo non responsabile delle tecnologie digitali.
Per l’elaborazione del presente documento ci si è avvalsi del materiale messo a disposizione dal Safer Internet Centre – Generazioni Connesse, dall’Amministrazione Scolastica e dalle strutture di supporto.

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.

Riflessione sui ruoli e sulle responsabilità di ciascuna figura del mondo scuola

Affinché l’ePolicy 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.

Di seguito vengono specificati i ruoli e le responsabilità di ciascuna figura del mondo scuola:

Il Dirigente Scolastico

il Dirigente Scolastico è il garante della sicurezza, anche online, di tutti i membri della comunità scolastica. Referente regionale eTwinning per l'Abruzzo la nostra Dirigente è adeguatamente formata sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR. Un ruolo importante, inoltre, è quello di promuovere la cultura della sicurezza online e, ove possibile, dare il proprio contributo all’organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull’ utilizzo positivo e responsabile delle TIC. Il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L’Animatore digitale

l’Animatore digitale, figura istituita a partire dall'introduzione del PNSD nelle scuole,insieme con il Team Diigitale, supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online. Facendo riferimento ai docenti del Team Digitale individuati appositamente, L'Animatore Digitale promuove percorsi di formazione interna all’Istituto negli

ambiti di sviluppo della “scuola digitale” (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell’ambito dell’educazione civica); monitora e rileva eventuali episodi o problematiche connesse all’uso delle TIC a scuola e,inoltre, controlla l'accesso e la fruizione da parte degli utenti autorizzati che accedono alla Rete della scuola con apposita password , per scopi istituzionali econsentiti (istruzione e formazione), nonchè alle Gsuite piattaforma utilizzata dai docenti del nostro istituto per la DDI e per la DaD.

Il Referente bullismo e cyberbullismo

“Ogni Istituto scolastico, nell’ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo” (Art. 4 Legge n.71/2017, “Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo” (permalink – file 1 LEGGE 71_2017 in allegato). Tale figura ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo e si avvale, soprattutto per la Scuola Secondaria di primo grado, della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, in quanto figura promotrice di progetti e percorsi formativi ad hoc, per studenti, colleghi e genitori, opportunamente supportata dal Team Digitale.

I Docenti

i Docenti hanno un ruolo centrale nel diffondere la cultura dell’uso responsabile delle TIC e della Rete. Nella progettazione didattica disciplinare (SSIG) e nei curricula disciplinari (SI - SP-SSIG) sono inseriti, laddove possibile, attività che promuovono l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l’uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete. A tal fine il nostro Istituto si è dotato di strumentazioni digitali con la partecipazione ai PON promossi dal Miur per la creazione di Ambienti di apprendimento innovativi, Smart Classes e, con l'emergenza sanitaria, all'allestimento di classi innovative 3.0. Tale apparato tecnologico viene gestito dal Team Digitale e dall'Animatore per una Didattica innovativa Integrata alla didattica tradizionale e per la DaD.

I docenti, inoltre,hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse, facendo riferimento al presente documento ePolicy, al regolamento d'istituto e al Patto di corresponsabilità educativa per quanto concerne le modalità di comunicazione e gestione delle stesse.

Il personale Amministrativo, Tecnico e Ausiliario (ATA

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. Diverse sono le figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Esiste, cioè, un **concreto coinvolgimento del personale ATA** . Il personale ATA è, all'interno dei singoli regolamenti d'Istituto, coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse

Gli Studenti e le Studentesse, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzano al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola **imparano a tutelarsi online**, e a tutelare i/le propri/e compagni/e e rispettarli/le; partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e si fanno promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I Genitori

i Genitori, in continuità con l'Istituto scolastico, sono partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. Vengono chiamati inoltre a sottoscrivere il presente documento ePolicy nonchè il Regolamento d'istituto ed il Patto di corresponsabilità.

Gli Enti educativi esterni e le associazioni

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola rappresentano un ruolo di stakeholders importante e si conformano alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC. Obiettivo dell'Istituto è quello di coinvolgerli maggiormente nella promozione di

comportamenti sicuri online e coinvolgerli nella protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

Nell'Istituto viene promossa la corresponsabilità educativa e formativa che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse.

In particolare, il 2° comma dell'art. 2048 c.c. così recita: *"I precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi e apprendisti nel tempo in cui sono sotto la loro vigilanza"*. Per i genitori, invece, bisogna considerare: il 1° comma dell'art. 30 della Costituzione *"è dovere e diritto dei genitori mantenere, istruire ed educare i figli, anche se nati fuori del matrimonio"*; il 1° comma dell'art. 2048 c.c. ai sensi del quale *"il padre e la madre o il tutore sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone soggette alla tutela, che abitano con essi (...)"*; l'art. 147 del c.c. *"l'obbligo di mantenere, istruire, educare e assistere moralmente i figli, nel rispetto delle loro capacità, inclinazioni naturali e aspirazioni (...)"*.

Dato questo quadro normativo, rispetto ad un profilo prettamente processuale anche in materia di bullismo e cyberbullismo (dunque non in via esclusiva), si può parlare di **tre tipologie di "culpa":**

- **culpa in vigilando:** concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (cosi come da art. 2048 del c.c.). Tale condizione è superabile se ci si avvale di una prova liberatoria di non aver potuto impedire il fatto (recita il terzo comma dell'art. 2048 c.c.: "le persone indicate nei commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto").
- **culpa in organizzando:** si riferisce ai provvedimenti previsti e presi dal Dirigente Scolastico ritenuti come non soddisfacenti e quindi elemento favorevole al verificarsi dell'eventuale incidente.
- **culpa in educando:** fa capo ai genitori i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.

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).

In coerenza con il percorso intrapreso e con le azioni che l'Istituto già pone in essere, la predisposizione di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione garantisce un migliore rapporto fiduciario fra scuola e famiglia, consente di distinguere i ruoli e le azioni da compiere e di attivare direttamente, a seconda della tipologia dei casi da segnalare, le autorità competenti collaborando con i servizi del territorio per la prevenzione e la gestione di quanto rilevato, in un'ottica di gestione condivisa degli interventi.

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

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

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

È necessario che il documento di ePolicy venga condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. Nello specifico è importante tener presente che:

- **condividere e comunicare il documento agli studenti e alle studentesse** significa dare loro una base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica; dare loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici; dare loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.
- **è importante condividere e comunicare il documento al personale scolastico** in modo da poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispostivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti;
- **è fondamentale condividere e comunicare il documento ai genitori** sul sito istituzionale della scuola, nonché tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.

Vi consigliamo, inoltre, di redigere una versione child friendly del documento per la comunicazione e la sensibilizzazione ai/lle bambini/e e ai/lle ragazzi/e. Nella comunicazione e condivisione dell'ePolicy è importante, infatti, valutare i vari target di riferimento (studenti/studentesse, docenti, genitori, personale amministrativo, collaboratori scolastici etc.) individuando di conseguenza i linguaggi, le modalità e i canali di comunicazione e condivisione più adatti.

È molto importante, inoltre, sottolineare che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

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.

A seconda dell'età dello studente o della studentessa, è molto importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione, allo scopo di promuovere una maggior consapevolezza circa l'utilizzo delle TIC e di Internet.

È opportuno, inoltre, valutare la natura e la gravità di quanto accaduto, al fine di **considerare la necessità di denunciare l'episodio** (con il coinvolgimento ad es. della Polizia Postale) o di garantire immediato supporto psicologico allo/la studente/ssa attraverso i servizi predisposti, qualora ciò fosse necessario.

1. Disciplina degli alunni

Le potenziali infrazioni in cui gli alunni potrebbero incorrere sono le seguenti:

- Un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare.
- L'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono.
- La comunicazione incauta e senza permesso con sconosciuti.
- Il collegamento a siti web non indicati dai docenti.

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo del bambino.

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

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario;

- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico.

2. Disciplina del personale scolastico

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

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non

connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;

- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile

con il ruolo professionale;

- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai

principi della privacy o che non garantisca un'adeguata protezione degli stessi;

- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e

degli accessi di cui possono approfittare terzi;

- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile

delle tecnologie digitali e di internet;

- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e

possibili incidenti;

- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno

agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni.

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

3. Disciplina dei genitori

In considerazione dell'età dei bambini (fino a 13 anni) e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico. Le situazioni familiari meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utlizzo del cellulare o dello smartphone;

- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;
- un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

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

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

- Integrazione della Policy con Regolamenti esistenti.

La policy richiede l'aggiornamento del Regolamento di Circolo con l'inserimento delle seguenti norme:

- UTILIZZO DEL LABORATORIO DI INFORMATICA, DELLE POSTAZIONI DI LAVORO E DELL' UTILIZZO DI INTERNET

L'uso della postazione di lavoro, sia per il personale della scuola sia per gli alunni, è soggetto alle seguenti condizioni

1. Divieti.

È vietato installare materiale protetto da copyright. È inoltre vietato l'uso della postazione di lavoro nell'ambito del servizio informativo dell'Istruzione o per i collegamenti a internet a scopi commerciali o di profitto personale e per attività illegali. Ricordando che la responsabilità delle operazioni compiute tramite una utenza è sempre del legittimo titolare della stessa, anche se compiute in sua assenza, la password ricevuta non deve essere comunicata a nessuno. Essa deve essere

memorizzata dall'utente che non deve trascriverla in nessun luogo. Ogni contatto ed operazione online (es. adesioni, iscrizioni, ecc.) che implica assunzione di impegni o responsabilità per conto della scuola deve essere autorizzata dal legale rappresentante dell'istituzione.

2. Uso personale.

E' consentito l'utilizzo della postazione di lavoro a fini personali solo se compatibile o funzionale al ruolo professionale svolto (ricerca di informazioni o documenti, approfondimenti culturali e dell'attualità, ecc.), purché, in aggiunta a quanto indicato nei punti precedenti, tale utilizzo:

1. non sia causa, diretta o indiretta, di disservizi dei sistemi elaborativi e dei servizi di collegamento dell'Amministrazione;

2. non sia causa di oneri aggiuntivi per l'Amministrazione;

3. non interferisca con le attività lavorative dell'utente, delle attività scolastiche o con altri obblighi dello stesso verso l'Amministrazione.

Al riguardo va tenuto ben presente che le risorse di rete e di memoria dei computer sono limitate. Tutti gli utenti hanno pertanto la responsabilità di farne un uso oculato evitando di sprecare deliberatamente dette risorse.

3. Uso didattico.

- Ogni allievo è direttamente responsabile della postazione assegnatagli per le ore in cui vi svolge lezione. Agli utenti è fatto assoluto divieto di cancellare, modificare in qualunque modo i file presenti sulla macchina o alterare il setup del sistema operativo o la configurazione dei programmi e dell'hardware della macchina.
- È fatto obbligo di adottare comportamenti idonei a non provocare danni o pericoli agli strumenti o alle attrezzature messi a disposizione. In caso contrario lo studente/utente dovrà porvi rimedio riparando o ripagando il danno e/o provvedendo alla pulizia e al riordino.
- Gli utenti sono tenuti a non prelevare o depositare informazioni, applicazioni o documenti che possano in qualsiasi modo arrecare danno a persone, cose o istituzioni.
- È vietato inserire file sul server o scaricare da internet

software non autorizzati o materiale soggetto a copyright o a diritti di proprietà intellettuale (software, file musicali, video, ecc.); l'insegnante controlla che questo divieto venga rispettato dagli allievi.

- Il riscontro di qualsiasi anomalia deve essere tempestivamente segnalato dagli alunni al docente e dal docente al responsabile del laboratorio.
- La connessione a internet dalla scuola prevede un login con password e gli studenti devono chiudere il collegamento dopo aver concluso la sessione di lavoro.
- Per utilizzare CD-ROM, DVD, penne USB o altri supporti di memorizzazione personali è necessario chiedere il permesso e sottoporli al controllo antivirus.
- L'utilizzo di videogame è vietato, a meno che non vi sia una finalità didattica del gioco, espressamente prevista dal docente.
- Si devono rispettare le regole di decenza e morali, evitare atti e comportamenti che possano recare offesa a cose, persone o istituzioni presenti o meno sulla rete.
- È fatto assoluto divieto di navigare in siti dai contenuti pornografici o contenenti scene di violenza, razzismo e sfruttamento dei minori.
- Si deve mantenere segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della scuola frequentata.
- Non si devono inviare a nessuno fotografie proprie o di amici.

I docenti che accompagnano gli allievi in laboratorio sono tenuti a controllare che vengano rispettati i divieti sopraelencati e che l'utilizzo delle risorse tecnologiche sia finalizzato agli intenti didattici previsti.

I docenti devono fare una mappa della disposizione degli allievi sulle macchine utilizzate e sono tenuti a far rispettare questa disposizione in ogni lezione, in modo che sia individuabile chi ha causato danni o infranto i divieti di cui sopra.

Ogni persona, docente o altro personale della scuola, che utilizza le strutture del laboratorio o comunque una postazione multimediale per accedere a internet deve segnalare sull'apposito registro la data, l'ora e la postazione da cui ha effettuato il collegamento.

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

1. É vietato agli alunni utilizzare il telefono cellulare e gli altri dispositivi elettronici e di intrattenimento (console portatili, mp3, ipod, ipad, notebook, fotocamera, videocamera, ecc.) durante ogni attività scolastica, in tutti i locali della scuola salvo specifiche deroghe autorizzate dal docente ai fini delle attività didattiche espressamente programmate e debitamente annotate su apposito registro.

2. I predetti dispositivi devono essere tenuti spenti e opportunamente custoditi e depositati nei borsoni, zaini, giacconi; giammai sul banco né tra le mani.

3. Eventuali esigenze di comunicazione tra gli alunni e le famiglie, in caso di urgenza, potranno essere soddisfatte mediante gli apparecchi telefonici della scuola; in alternativa il docente potrà concedere l'autorizzazione all'uso del cellulare, previa richiesta formale da parte dell'alunno e verifica preventiva da parte del docente che l'altro interlocutore sia il genitore e/o chi ne fa le veci.

4. Nel caso in cui lo studente sia sorpreso a utilizzare il cellulare o qualsiasi altro dispositivo durante una verifica scritta (compiti in classe, test, ecc.), la stessa sarà ritirata e non dovranno essere previste prove di recupero.

5. All'interno di tutti i locali della scuola, ivi compresi corridoi, atri, servizi, palestre, aule e laboratori sono vietate riprese audio e video di ambienti e persone, salvo in caso di esplicita autorizzazione del docente responsabile.

6. Il divieto di utilizzare telefoni cellulari durante lo svolgimento di attività di insegnamento e di apprendimento opera anche nei confronti del personale docente, in considerazione della necessità di assicurare all'interno della comunità scolastica le migliori condizioni per uno svolgimento sereno ed efficace delle attività didattiche, unitamente all'esigenza educativa di offrire ai discenti un modello di riferimento esemplare da parte degli adulti.

7. Durante l'orario di servizio è consentito al personale scolastico l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente. Ogni altro dispositivo elettronico può essere utilizzato solo se richiesto dalle attività di servizio svolte.

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.

- Monitoraggio dell'implementazione della Policy e suo aggiornamento.

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolta ogni anno, con l'alternarsi delle classi quarte e quinte. Le modifiche del documento vanno discusse con tutti i membri del personale docente. Il monitoraggio del documento prevede anche una valutazione della sua efficacia a partire dagli obiettivi specifici che lo stesso si pone (promozione delle competenze digitali e dell'uso delle TIC nei percorsi educativi e didattici, prevenzione e gestioni dei rischi online etc...).Tale monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale e dai docenti delle classi, tramite questionari e conversazioni. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti.

L'aggiornamento della policy sarà curato dal Dirigente scolastico, dall'Animatore digitale, dagli Organi Collegiali, a seconda degli aspetti considerati.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

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

Azioni da svolgere nei prossimi 3 anni:

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

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.

Inserita nelle otto Competenze chiave di cittadinanza attiva indicate dal Consiglio di Lisbona nel marzo 2000, la competenza digitale viene così definita all'interno della "Raccomandazione del Parlamento europeo e del Consiglio" del 18 dicembre 2006, relativa a competenze chiave per l'apprendimento permanente (2006/962/CE):
"La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet".
Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali 2012:
‹‹La competenza digitale è ritenuta dall'Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d'oggi. L'approccio per

discipline scelto dalle Indicazioni non consente di declinarla con le stesse modalità con cui si possono declinare le competenze chiave nelle quali trovano riferimento le discipline formalizzate. Si ritrovano abilità e conoscenze che fanno capo alla competenza digitale in tutte le discipline e tutte concorrono a costruirla. Competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.››

L'istituto aderisce dall' a.s. 2015/2016 al progetto ministeriale "Programma il futuro", coinvolgendo nella sperimentazione del coding le classi presenti nella scuola ed integrando così le competenze digitali già previste dalle Indicazioni Nazionali, attraverso la promozione dello sviluppo negli alunni del "pensiero computazionale".
Il pensiero computazionale è un processo mentale per la risoluzione di problemi costituito dalla combinazione di metodi caratteristici e di strumenti intellettuali, entrambi di valore generale.

Con l'emergenza sanitaria, la scuola si è impegnata nel creare ambienti di apprendimento innovativi per portare avanti la didattica quotidiana in modalità blended. A tal fine si è dotata di strumenti di innovazione tecnologica ed ha utilizzato metodologie didattiche non tradizionali per promuovere l'acquisizione delle competenze.Sono state predisposte Classi virtuali attraverso l'utilizzo della Suite di Google e ambienti virtuali di condivisione dei materiale: Drive, Argo, eTwinning.Ciò a comportato la creazione di una Netiquette da parte degli studenti per renderli consapevoli del processo di apprendimento. Il documento è parte integrante del regolamento scolastico. L'Istituto si è inoltre dotato di un curricolo digitale trasversale alle varie discipline e progettato ad hoc a seconda del target di riferimento (scuola primaria, secondaria di I°)

Come già evidente nella definizione iniziale delle Raccomandazioni Europee, le competenze digitali richiamano diverse dimensioni sulle quali sarà possibile lavorare in classe, in un'ottica che integra la dimensione tecnologica con quella cognitiva ed etica (Calvani, Fini e Ranieri 2009):

- **dimensione tecnologica**: è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un'adeguata comprensione della "grammatica" dello strumento.
- **dimensione cognitiva:** fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità.
- **dimensione etica e sociale:** la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone un po' più l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di

coloro con cui comunichiamo online.

Premesso ciò, è opportuno fare riferimento ad un framework comune per le competenze digitali e l'educazione ai media degli studenti e delle studentesse. I documenti più importanti per progettare e implementare un buon curricolo sulle competenze digitali a cui fare riferimento sono:

Piano Scuola Digitale (PNSD), in particolar modo il paragrafo 4.2. su "Competenze e contenuti": è il documento di indirizzo del Ministero dell'Istruzione, dell'Università e della Ricerca per il lancio di una strategia complessiva di innovazione della scuola italiana e per un nuovo posizionamento del suo sistema educativo nell'era digitale (Permalink – File 2 Piano Scuola Digitale).

-Sillabo sull'Educazione Civica Digitale**: ha** lo scopo di inquadrare il corpus di temi e contenuti che sono alla base dello sviluppo di una piena cittadinanza digitale degli studenti attraverso il percorso educativo.

-DigComp 2.1.: "Il quadro di riferimento per le competenze digitali dei cittadini", con otto livelli di padronanza ed esempi di utilizzo (Permalink – File 3 DigComp).

-Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente (C189/9, p. 9): documento in cui vengono specificate le conoscenze, le abilità e gli atteggiamenti essenziali legati a tale competenza

Il DigComp, in particolare, è diventato un riferimento per lo sviluppo e la pianificazione strategica di iniziative sulle competenze digitali, sia a livello europeo sia nei singoli stati membri dell'Unione. Il documento prevede:

- Aree di competenze individuate come facenti parte delle competenze digitali;
- Descrittori delle competenze e titoli pertinenti a ciascuna area (21 competenze);
- Livelli di padronanza per ciascuna competenza (i livelli sono 8);
- Conoscenze, abilità e attitudini applicabili a ciascuna competenza;
- Esempi di utilizzo sull'applicabilità della competenza per diversi scopi.

Le aree di competenza individuate dal Digcomp sono, nello specifico:

Area 1: "Alfabetizzazione e dati"

L'area s'inquadra nella dimensione "informazionale" o "cognitiva" delle competenze digitali. Essa è relativa alla capacità di cercare, selezionare, valutare e riprocessare le informazioni in Rete. Nello specifico, per quest'area si dovrebbe puntare a sviluppare in bambini e ragazzi le seguenti competenze: 1. Navigare, ricercare e filtrare dati, informazioni e contenuti digitali; 2. Valutare e gestire dati, informazioni e contenuti digitali; 3. Saper riconoscere e sapersi difendere da contenuti

dannosi e pericolosi in Rete (es. app, giochi online, siti non adatti ai minori, materiale pornografico e pedo-pornografico etc.).

Area 2: "Comunicazione e collaborazione"

Quest'area fa riferimento a quelle competenze volte a riconoscere le giuste ed appropriate modalità per comunicare e relazionarsi online:

1. Saper interagire con gli altri attraverso le tecnologie digitali;

2. Essere consapevoli nella condivisione delle informazioni in Rete;

3. Essere buoni "cittadini digitali";

4. Collaborare adeguatamente con gli altri attraverso le tecnologie digitali;

5. Conoscere le "Netiquette", ovvero le norme di comportamento online;

6. Saper gestire la propria "identità digitale".

Area 3: "Creazione di contenuti digitali"

Quest'area fa riferimento alle capacità di "valutare le modalità più appropriate per modificare, affinare, migliorare e integrare nuovi contenuti e informazioni specifici per crearne di nuovi e originali" (cfr. DigComp 2.1.). Le specifiche competenze digitali che andranno sviluppate in questo caso sono:

1. Creare e modificare contenuti digitali in diversi formati per esprimersi attraverso mezzi digitali;

2. Modificare, affinare, migliorare e integrare informazioni e contenuti all'interno di un corpus di conoscenze esistente per creare conoscenze e contenuti nuovi, originali e rilevanti;

3. Capire come il copyright e le licenze si applicano ai dati, alle informazioni e ai contenuti digitali.

Area 4: "Sicurezza"

Quest'area è parte di una dimensione più generale definita come "benessere digitale" che include la necessità di salvaguardare i propri dati personali e rispettare le regole nel trattare i dati altrui. Nello specifico, bisognerebbe puntare a sviluppare in bambini e ragazzi le seguenti competenze:

1. Imparare a proteggere i dispositivi e i contenuti digitali e comprendere i rischi e le minacce presenti negli ambienti digitali. Conoscere le misure di sicurezza e protezione e tenere in debita considerazione l'affidabilità e la privacy;

2. Proteggere i dati personali e la privacy negli ambienti digitali. Capire come utilizzare e condividere informazioni personali proteggendo se stessi e gli altri dai danni. Comprendere che i servizi digitali hanno un "regolamento sulla privacy" per informare gli utenti sull'utilizzo dei dati personali raccolti;

3. Conoscere (ed esercitare) i propri diritti in termini di privacy e sicurezza.

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

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

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

La professione docente è complessa e pertanto richiede competenze diverse ed integrate, fra queste anche quelle di tipo digitale. Le TIC, infatti, dovrebbero essere usate dagli insegnanti ad integrazione della didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli studenti e le studentesse della classe, anche delle persone con disabilità (in chiave inclusiva).

Di conseguenza, gli insegnanti dovrebbero avere o raggiungere un buon livello di formazione in merito all'utilizzo e l'integrazione delle TIC nella didattica, tenendo presente l'immagine che fornisce in merito il DigComp: "imparare a nuotare nell'oceano digitale".

La mission dell'Istituto Comprensivo è quella di portare tutti gli alunni ad avere un livello di "sopravvivenza" nel digitale e per fare ciò anche i docenti devono essere formati e raggiungere un livello di competenze digitali tale da permettere loro di istruire gli alunni e di svolgere una didattica innovativa, creativa e motivante.

La metafora fornita dal documento indica che è necessario sapersi destreggiare, partendo dai compiti semplici (es.: individuare i fabbisogni informativi; trovare dati, informazioni e contenuti attraverso una semplice ricerca in ambienti digitale etc.) per arrivare ai compiti complessi che presentano molti fattori di interazione (ad es.: creare nuove app o piattaforme per navigare, ricercare e filtrare portali e offerte).

È su tali premesse che l'Istituto, attraverso il collegio dei docenti, riconoscere e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (ad es. con l'aiuto dell'animatore digitale) dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online), purché restino coerenti con il piano di formazione.

Da qualche anno a questa parte, l'Istituto organizza corsi di alfabetizzazione informatica per i docenti nuovi arrivati e corsi via via più specializzanti per i docenti dell'Istituto sull'uso dei

dispositivi mobili per la didattica innovativa, utilizzo di piattaforme dedicate ed ambienti di apprendimento virtuali per il raggiungimento delle competenze.

Fondamentale, infatti, che vi sia attenzione all'uso delle TIC nella didattica: un loro utilizzo strutturato e integrato non solo può rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi, ma permette al docente di guidare studenti e studentesse rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento al di fuori della scuola. Inoltre, permettono di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona.

La competenza digitale, oggi, è imprescindibile per i docenti così come per studenti e studentesse e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa e in grado di venire incontro ai nuovi stili di apprendimento.

Gli insegnanti, dunque, dovrebbero essere pronti a cogliere tale sfida anche grazie alla possibilità di formazione permanente offerta loro in primis dall'Istituto scolastico, in modo da rispondere ai diversi bisogni formativi della classe.

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.

Nell'ottica di creare ulteriore sinergia fra scuola, studenti/studentesse e famiglie, di promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo, è necessario e auspicabile che i docenti tutti dell'Istituto scolastico seguano un percorso formativo specifico ed adeguato che abbia ad oggetto non solo l'uso responsabile e sicuro della Rete ma anche i rischi legati a quest'ultime.

Formare i docenti sulle tematiche in oggetto vuol dire non pensare esclusivamente all'alfabetizzazione ai media ma anche considerare la sfera emotiva e affettiva degli studenti e delle

studentesse che usano le nuove tecnologie. Essi/e, infatti, comunicano, esprimono se stessi e sviluppano l'identità personale e sociale, attraverso i dispositivi tecnologici che sempre di più consentono loro di poter entrare in contatto con il mondo che li circonda. Prestare attenzione a questi aspetti significa dare loro gli strumenti per poter educare ragazzi e ragazze alle emozioni in contesto onlife e quindi modulare e gestire i propri ed altrui comportamenti, favorendo e promuovendo forme di convivenza civile.

Per tali ragioni, l'Istituto prevede specifici momenti di formazione permanente per gli insegnanti che mettono al centro i temi in oggetto, considerando anche percorsi di autoaggiornamento personali o collettivi, iniziative seminariali con professionisti-esperti interni (si pensi al supporto dell'Animatore digitale) ed esterni alla scuola, giornate-settimane di approfondimento in accordo con la rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc…), le amministrazioni comunali, i servizi socio-educativi e le associazioni/enti presenti. Si pensi all'inserimento di tali azioni programmatiche nel Piano triennale dell'offerta formativa.

Sarebbe auspicabile pensare a momenti formativi di approfondimento (progetti specifici, laboratori, eventi, giornate, etc, …) con la famiglia e gli/le studenti/studentesse in modo da sensibilizzare l'intera comunità educante sia su un corretto uso delle tecnologie digitali sia sulle potenzialità della Rete.

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

Si potrebbe anche pensare ad un cronoprogramma che consideri il triennio scolastico, in un'ottica di vera e propria programmazione, con azioni specifiche. Per esempio:

- **Analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;**
- **Promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse".**
- **Promuovere la partecipazione dei genitori ed alunni a corsi di formazione che abbiano per oggetto le Tic e i progetti promossi da Generazioni Connesse.**
- **Monitorare le azioni svolte per mezzo di specifici momenti di valutazione;**
- **Organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.**

Potrebbe essere predisposta un'area specifica sul sito dell'Istituto con materiali formativi per gli insegnanti. Nella sezione, potrebbero essere messi a disposizione materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet, prevedendo possibilità e modalità di condivisione fra gli insegnanti.

Sempre sul sito istituzionale della scuola, sarebbe auspicabile includere link e materiali informativi

del progetto "**Generazioni connesse**", a partire dall'inserimento del link del progetto: www.generazioniconnesse.it/ dove trovare ulteriori approfondimenti, spunti aggiornamenti e strumenti didattici utili da usare con gli studenti e le studentesse, per ciascun grado di scuola.

Una parte del corpo docente ha partecipato a corsi di formazione anche nell'ambito di piani nazionali. Sono in corso iniziative di formazione organizzate dall'istituzione o dalle scuole associate in rete. Il corpo docente più giovane possiede generalmente una buona base di competenze e, nel caso delle figure di sistema, si dispone anche di una preparazione specialistica. Il resto del collegio dovrebbe aggiornarsi per mantenere la propria formazione al passo con i tempi, specie in considerazione dell'impegno che l'Istituto sta profondendo proprio nel corrente a.s. per Rinnovare la dotazione multimediale di ciascuno dei sei plessi (PON 2014-2020 - realizzazione di infrastrutture di rete LAN/WLAN; creazione di laboratori multimediali). Quattro docenti dell'Istituto hanno partecipato alla selezione nazionale per l'assegnazione di borse di studio sulle competenze digitali conseguendo il titolo di Formatori della Didattica Innovativa. Essi sono iscritti al Registro Internazionale IET (Innovative Educational Trainers) con l'Ente Certificatore EIPASS. In seguito l'Istituto si è accreditato come centro esami Eipass e sta formando alunni per la certificazione Junior for School.

Per la formazione specifica dei docenti sull'utilizzo delle TIC nella didattica, si prevedono momenti di autoaggiornamento, di formazione personale o collettiva anche all'interno dell'istituto, tramite la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo.

Come anticipato, l'Istituto partecipa alle iniziative dedicate al digitale:

- Progetto "Programma il futuro"
- Progetto "Generazioni Connesse"
- Coding e pensiero computazionale
- Piano Nazionale Scuola Digitale
- Abruzzo Scuola Digitale
- Rete di scuole Digit School
- Eipass Junior For School
- Safe Internet Day (prevenzione e sicurezza informatica – cyberbullismo)

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.

L'Istituto intende attivare 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 previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate, ricavato dai siti specializzati e dalle forze dell'ordine.

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 cyber bullismo.

La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (Policy e-safety) per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un utilizzo non corretto di internet.

Il nostro piano d'azioni

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

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

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

personali.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea

La scuola è chiamata ogni giorno a costruire le condizioni per un futuro migliore delle nuove generazioni. Questa sfida riguarda anche il "corretto trattamento dei dati personali", presupposto necessario per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza.

Nelle scuole di ogni ordine e grado vengono trattate giornalmente numerose informazioni sugli studenti e le studentesse, sulle loro famiglie, sui loro problemi sanitari o di disagio sociale, o ad esempio sulle abitudini alimentari. A volte può bastare una lettera contenente dati sensibili (quelli più delicati) di un minorenne, o un avviso scolastico con riferimenti indiretti sulle condizioni di salute degli/lle studenti/esse, per violare anche involontariamente la riservatezza e la dignità di una persona.

Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali che si trovano a trattare, in particolare quando sono coinvolti soggetti minorenni.

La protezione dei dati personali è, infatti, 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 particolare, la scuola non ha solo il compito di tutelare la privacy degli/lle studenti/esse e delle loro famiglie, ma anche quello di informare e soprattutto rendere consapevoli gli/le studenti/esse di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri.

In questo paragrafo della vostra ePolicy vi invitiamo, quindi, a riflettere sul tema del trattamento dei dati personali a scuola, con particolare riferimento all'uso delle tecnologie digitali, e indicare le misure che intendete 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.

La diffusione sempre maggiore di smartphone tra i giovanissimi, l'uso di tablet a scopo didattico, la condivisione online di contenuti didattici, l'uso del registro elettronico, l'eventualità di gruppi whatsapp tra studenti/esse, genitori, docenti o tra insegnanti e studenti/esse, obbliga la scuola ad avere un'attenzione particolare

non solo alla privacy in generale, ma anche alla gestione della privacy legata all'uso dei nuovi dispositivi. La velocità, l'immediatezza con cui si risponde ai messaggi o si condividono foto o video, può far perdere il controllo di dati personali e mettere a rischio la reputazione e la sicurezza dei soggetti coinvolti.

Ma cosa si intende quando si parla di "dati personali"?

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.

Fra questi, particolarmente importanti sono:

- i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);
- i dati rientranti in particolari categorie: si tratta dei dati cosiddetti sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- i dati relativi a condanne penali e reati: si tratta dei dati cosiddetti giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Con l'evoluzione delle tecnologie digitali, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via Internet o telefono) e quelli che consentono la geo-localizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti di una persona.

Chi sono le parti in gioco quando parliamo di "protezione dei dati personali"?

- L'interessato è la persona fisica alla quale si riferiscono i dati personali (art.

4, paragrafo 1, punto 1), del Regolamento UE 2016/679);

- Il titolare è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico, privato o l'associazione che adotta le decisioni sugli scopi e sulle modalità del trattamento (art. 4, paragrafo 1, punto 7), del Regolamento UE 2016/679);
- Il responsabile è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati (art. 4, paragrafo 1, punto 8), del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. sub-responsabile (art. 28, paragrafo 2).

Cosa s'intende per "trattamento dei dati"?

Trattamento è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali.

Ad esempio: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, par. 1, punto 2, del Regolamento (UE) 2016/679).

I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati.

Quali sono gli obblighi delle scuole in tema di "protezione dei dati personali"?

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti non sono tenute a chiedere il consenso degli/lle studenti/esse.

Alcune categorie di dati personali degli/lle studenti/esse e delle famiglie, come quelli sensibili e giudiziari, devono essere trattate con estrema cautela, nel rispetto di specifiche norme di legge, verificando in primis non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire.

Esempi di violazione sono il trattamento dei dati senza aver fornito all'interessato un'adeguata informativa o senza aver ottenuto uno specifico e libero consenso,

qualora previsto.

In tali casi la persona interessata (studente/essa, professore, etc.) può presentare al Garante per la Protezione dei dati personali un'apposita "segnalazione" gratuita o un "reclamo" (più circostanziato rispetto alla semplice segnalazione e con pagamento di diritti di segreteria).

Le scuole, sia pubbliche che private, hanno l'obbligo di informare (tramite apposita informativa) gli interessati delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento. Gli interessati non sono solo gli/le studenti/esse, ma anche le famiglie e gli stessi professori. È importante, inoltre, che le scuole verifichino i loro trattamenti, controllando se i dati siano eccedenti rispetto alle finalità perseguite.

In sintesi, vi elenchiamo i punti necessari da soddisfare per rendere compliant ogni Istituto Scolastico al Regolamento UE 2016/679:

- Redigere e mantenere un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti.
- Valutazione dei rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili. Le istituzioni scolastiche pubbliche e private possono trattare anche dati sensibili, come ad esempio dati relativi alle origini razziali per favorire l'integrazione degli/lle alunni/e, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli/lle alunni/e, come i dati vaccinali con le Asl.
- Analisi di processo sulla raccolta/gestione del consenso: occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio, all'interno di modulistica o sul proprio sito web istituzionale. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice e chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, ma devono ad esempio adeguare tutta la modulistica al Regolamento UE 2016/679 e predisporre una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.
- Adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti:
- **analisi del sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati:**

a) valutazione di migrazione del sito da suffissi gov.it (non più validi per le

istituzioni scolastiche secondo la determina n. 36 del 12 febbraio 2018) a suffissi edu.it;

b) progettazione del nuovo sito secondo i concetti di privacy by default e by design;

c) utilizzo del protocollo HTTPS (l'Hypertext Transfer Protocol Secure è un protocollo per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati online);

d) utilizzo di un sistema di cifratura quando il trattamento di dati lo richiede (ovvero oscurare il dato per renderlo incomprensibile a coloro che non hanno i codici per accedervi, mediante la "crittografia" e, quindi, l'uso di un algoritmo di cifratura);

e) sistema di backup (sistema che permette di salvare regolarmente i dati; ripristinare eventuali file modificati o rimossi per errore dalla rete; garantire la presenza di una copia di sicurezza di tutti i file importanti);

f) piano di disaster recovery (insieme di misure che permettono agli apparati di Information technology di superare situazioni di emergenza, ovvero di impedire che imprevisti accidentali o incidenti possano compromettere il funzionamento delle strutture);

- **proposte di messa in sicurezza della intranet scolastica:**

a) sulle reti Wi-fi installate;

b) utilizzo di white list per la navigazione (sistemi di filtraggio dei contenuti);

c) utilizzo di un proxy (un server che, ad esempio, si interpone nel flusso di comunicazione fra un computer e un sito Internet, eliminando il collegamento diretto fra il client e il server di destinazione. Permette di fornire un maggiore anonimato durante la navigazione in Rete, funziona da antivirus e memorizza una copia locale degli elementi web).

e) uso di un firewall hardware ;

f) istituire corsi di formazione destinati ai responsabili, agli incaricati ed eventualmente ai sub-incaricati del trattamento.

Qualche anno fa il Garante ha pubblicato un utile vademecum "La scuola a prova di privacy" che offre agli insegnanti e ai dirigenti una guida per gestire correttamente le questioni legate alla diffusione e al trattamento dei dati personali degli studenti e delle famiglie. Il documento è stato elaborato prima dell'applicazione del Regolamento UE 679/2016, avvenuta il 25 maggio 2018 e di ciò bisogna tenere conto nel momento in cui lo consulterete. Rimane, in ogni modo, un riferimento tuttora molto utile per aiutare docenti, famiglie, studenti/esse e la stessa amministrazione scolastica a muoversi più agevolmente

nel delicato mondo della protezione dei dati personali. Vi consigliamo, quindi, di consultarlo nella stesura di questo paragrafo dell'ePolicy.

Ad esempio, il vademecum ricorda che non è consentito evidenziare nelle comunicazioni pubbliche della scuola lo stato di morosità delle famiglie rispetto al pagamento della mensa scolastica o di altre somme dovute, né rendere noto lo svolgimento di prove d'esame in forma differenziata da parte di studenti con handicap o disturbi dell'apprendimento, né divulgare i nomi di studenti che si sono resi responsabili di atti di bullismo o vandalismo: tutte le comunicazioni su questioni specifiche di interesse individuale vanno indirizzate esclusivamente agli interessati ed al personale preposto.

La Liberatoria: quali dati deve contenere?

La scuola non è tenuta a richiedere alle famiglie l'autorizzazione alle riprese fotografiche e video (ad es. in caso di gite scolastiche o recite) solo se esse sono realizzate a fini personali e non a fini di pubblicazione o divulgazione: attenzione dunque ai siti web della scuola, ma anche alle pagine Facebook o a whatsapp perché si tratta di divulgazione e necessita di autorizzazione degli interessati.

In generale il Garante per la protezione dei dati personali stabilisce che "le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano. Spesso le scuole utilizzano nella loro attività quotidiana dati delicati - come quelli riguardanti le origini etniche, le convinzioni religiose, lo stato di salute - anche per fornire semplici servizi, come ad esempio la mensa. È bene ricordare che nel trattare queste categorie di informazioni gli Istituti scolastici devono porre estrema cautela, in conformità al "Regolamento sui dati sensibili" adottato dal Ministero dell'Istruzione".

Famiglie e studenti hanno il diritto di conoscere quali informazioni sono trattate dall'Istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

In allegato all'ePolicy i modelli di liberatoria che l'Istituto utilizza o intende utilizzare, modelli che devono essere conformi alla normativa vigente, in materia di protezione dei dati personali.

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.

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.

Date queste premesse, il gruppo di lavoro incaricato di definire l'ePolicy dovrebbe interrogarsi su come garantire tale diritto a scuola e in quali modalità a tutti gli/le studenti/esse.

Il primo passo è conoscere il più possibile l'infrastruttura tecnologica dell'Istituto, in modo da poterla sfruttare e potenziare in modo coerente con le necessità dei docenti e la visione che la scuola ha rispetto all'uso delle ICT. Per questo è necessario coinvolgere l'animatore digitale e il tecnico informatico.

Infatti, la pianificazione che riguarda l'acquisizione, la gestione e il mantenimento dell'infrastruttura e dei device non può essere pensata se non all'interno della strategia che la scuola intende adottare attraverso l'ePolicy. È necessario,

dunque, tenere in considerazione due aspetti:

- **lo status quo**, cioè la disponibilità attuale di tecnologia nella scuola e come rendere l'infrastruttura sicura, accessibile ma anche funzionante e adatta allo scopo. Per questo può essere utile avviare progetti pilota che permettano una sperimentazione e un acquisto più razionale e dilazionato degli strumenti, raccordandosi sempre con l'animatore digitale.
- **l'analisi dei bisogni della scuola** (o del plesso), in relazione alle reali esigenze didattiche e agli obiettivi prefissati. Questo permette di pianificare e di cogliere eventuali occasioni che possono presentarsi sotto forma di bandi, donazioni o finanziamenti.

Ad esempio, nel caso in cui la scuola dovesse provvedere ad un aggiornamento dell'infrastruttura di rete, dovrebbe pensare a lungo termine e permettere l'accesso a Internet a tutte le classi, attraverso una rete Wi-fi adeguata al numero di studenti e in grado di supportare il traffico dati generato da un numero elevato di utenti. Il PNSD prevede che "ogni scuola debba essere raggiunta da fibra ottica, o comunque da una connessione in banda larga o ultra-larga, sufficientemente veloce per permettere, ad esempio, l'uso di soluzioni cloud per la didattica e l'uso di contenuti di apprendimento multimediali e che le strutture interne alla scuola devono essere in grado di fornire, attraverso cablaggio LAN o wireless, un accesso diffuso, in ogni aula, laboratorio, corridoio e spazio comune". Per questo è necessario non solo il monitoraggio di opportunità in tal senso tramite bandi PON o europei, ma anche interloquire con le amministrazioni locali, spesso sensibili alle questioni del digital mismatch (il divario tra le competenze in ambito ICT richieste dalle imprese e quelle possedute dai giovani italiani). Tale adeguamento è necessario anche in ottica di un potenziamento degli strumenti didattici e laboratoriali necessari a migliorare la formazione e i processi di innovazione delle istituzioni scolastiche e all'adozione di strumenti organizzativi e tecnologici che permettano un'amministrazione trasparente, la condivisione di dati e la dematerializzazione degli atti, oltre al fondamentale scambio di informazioni tra dirigenti, docenti, famiglie e studenti/esse, permesso, ad esempio, dal registro elettronico.

Un ambiente sicuro anche online

In inglese esistono due termini per parlare di sicurezza: il primo termine è safety e riguarda la prevenzione dei rischi, a partire dalla consapevolezza, conoscenza e preparazione per un uso consapevole delle tecnologie digitali (ed è questo l'approccio del progetto "Generazioni Connesse"). L'altro termine è security che, in relazione ad Internet e ai media, si riferisce a tutte quelle risorse tecnologiche che rendono sicuro l'ambiente digitale, dall'antivirus al firewall, da un protocollo di trasmissione dei dati sicuro (https) all'aggiornamento di software e sistemi operativi.

La scuola deve dunque considerare l'ambiente online alla stregua dell'ambiente fisico e valutarne tutti gli aspetti legati alla sicurezza nel momento in cui permette a studenti/esse e docenti l'accesso alla rete tramite i dispositivi della scuola, tramite la rete scolastica o tramite i dispositivi personali nel caso del BYOD (Bring your own device) di cui si parlerà in modo specifico più avanti.

In riferimento alla security non è sufficiente prestare attenzione all'infrastruttura hardware e alla rete (wireless e non), ma è necessario considerare anche la sicurezza di tutti gli aspetti che riguardano la gestione degli account degli utenti (in modo differenziato tra studenti, insegnanti e personale amministrativo), il filtraggio dei contenuti (possibilmente in modo differenziato in base all'età) e gli aspetti legali in relazione prevalentemente alla privacy.

Infine, nell'ePolicy andrebbe inserito oppure allegato un regolamento d'Istituto sull'uso delle TIC. Per le scuole che hanno già sviluppato una "Politica di Uso Accettabile delle tecnologie a scuola" (PUA) è sufficiente aggiornare quest'ultima e allegarla.

L'annosa questione della tecnologia che non funziona

Per superare la diffidenza nei confronti delle tecnologie a scuola e il divario nell'accesso, è necessario andare oltre la possibile prima barriera che ne inibisce un uso efficace da parte di tanti docenti: i problemi tecnici e la scarsa familiarità con la strumentazione.

Per affrontare proattivamente la questione sarebbe auspicabile che la scuola provvedesse a pianificare interventi periodici di manutenzione e tenesse anche un registro delle problematiche incontrate per poter stilare una classifica dei problemi più frequenti. Questo aspetto è fondamentale per formare gli insegnanti e permettere loro di affrontare e risolvere in autonomia tutte quelle situazioni e casistiche di mal funzionamento dei dispositivi che si possono presentare nella quotidianità. La parola d'ordine per quanto riguarda le tecnologie è sempre: "formazione". Formazione non solo sull'uso delle tecnologie digitali nella didattica, ma anche sul funzionamento e sull'uso stesso della tecnologia in sé. Sarebbe opportuno a tal fine coinvolgere il tecnico della scuola, in collaborazione con l'animatore digitale e qualche docente che per studio o passione ha conoscenze più tecniche da poter condividere coi colleghi.

La formazione dovrebbe anche aiutare a familiarizzare con i dispositivi, laddove ci fossero incertezze e difficoltà. Suggeriamo, inoltre, di pensare anche a soluzioni diverse dal semplice uso della LIM o delle tecnologie scolastiche. Ad esempio, si pensi, agli atelier digitali e creativi, alle "aule digitali" realizzate in tante scuole con i contributi PON-MIUR. Aule pensate per avere, ad esempio, un tappeto digitale e permettere un approccio diverso e più integrato della tecnologia nella didattica.

Anche il BYOD può essere un ottimo strumento, come si vedrà più avanti: oltre allo smartphone, possono essere utilizzati in gruppo tablet o computer personali, in modo che le tecnologie possano diventare anche strumenti per collaborare insieme e non solo, come talvolta accade, per alienarsi rispetto agli altri.

Nel caso di uso degli smartphone ciò è possibile previo accordo con studenti/esse e genitori.

Il regolamento sull'uso delle tecnologie a scuola

Indipendentemente dalle scelte dell'Istituto rispetto alla tipologia di strumentazione e alle impostazioni di connessione, è necessario dotarsi di un regolamento d'Istituto sull'uso delle TIC da allegare alla ePolicy. Per meglio definire i confini dei due strumenti, l'ePolicy è il documento in cui in modo discorsivo e generale vengono descritti gli aspetti necessari per dotarsi di una visione e comprensione del fenomeno e delle sue potenzialità in ambito didattico; le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali. Nel regolamento sull'uso delle tecnologie andremo ad elencare in modo puntuale le regole di ingaggio nell'utilizzo della strumentazione tecnologica della scuola, ovvero le azioni che docenti, personale scolastico e studenti/esse possono e non possono compiere quando si connettono alla Rete e/o accedono a un device. Tale regolamento deve prevedere anche una parte sull'uso della strumentazione personale a scuola, sia nel caso del BYOD, qualora i docenti proponessero ai propri studenti l'uso di device personali (tablet, PC o smartphone) in classe, ma anche regole per quanto riguarda la presenza degli smartphone a scuola, non a supporto delle attività didattiche.

Gli Istituti già dotati di una PUA (Politica d'Uso Accettabile), possono aggiornare tale documento e allegarlo all'ePolicy e verrà considerato in modo equivalente al regolamento.

Il regolamento, dunque, deve prevedere una parte dedicata all'uso di Internet in cui gli studenti si impegnano a:

- *utilizzare la rete nel modo corretto*
- *rispettare le consegne dei docenti*
- *non scaricare materiali e software senza autorizzazione*
- *non utilizzare unità removibili personali senza autorizzazione*
- *tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo*
- *durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente*

per svolgere le attività didattiche previste

- *segnalare immediatamente materiali inadeguati ai propri insegnanti.*

I docenti si impegnano a:

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

Ricordiamo, come evidenziato nel modulo 2, che la legge Ferrara, la legge 71 del 29 maggio 2017, chiede alle scuole di aggiornare il patto di corresponsabilità, per cui andrebbe inserito un punto specifico relativo all'uso della connessione Internet della scuola. La scuola dovrebbe informare che si farà carico di tutte le precauzioni necessarie per garantire agli/lle studenti/esse l'accesso a materiale appropriato, ma che allo stesso tempo non può essere responsabile per l'accesso autonomo da parte degli/lle studenti/esse a materiali inadeguati e potenzialmente dannosi trovati online.

Il curricolo scolastico prevede che gli/le studenti/esse imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le ICT. Oggi è anche fondamentale dotare gli/le studenti/esse delle competenze necessarie ad affrontare la complessità del mondo dell'informazione, che ormai richiede di essere in grado di destreggiarsi tra notizie e fake news, discussioni online e discorsi d'odio (hate speech). Inoltre, attraverso programmi come eTwinning, si offrono sia agli/lle studenti/esse che agli insegnanti opportunità di scambi culturali con gli/le studenti/esse di altri Paesi ed è dovere della scuola regolare e definire modalità di coinvolgimento che facilitino tali percorsi.

Non è un caso che eTwinning richieda una ePolicy alle scuole per entrare nel programma.

Se la scuola fornisce agli studenti un indirizzo di posta elettronica personale (eventualmente collegato al cloud della scuola), attivo per il tempo di permanenza nell'Istituto, questo andrà regolato nella PUA: gli studenti dovranno utilizzarlo per accedere alle piattaforme e-learning e tutte le attività ICT della scuola stessa. Nel documento andrà anche definita la scadenza programmata degli accessi (tipicamente al 31 agosto dell'anno di fine percorso scolastico). Lo stesso dicasi per gli account di docenti e personale della scuola.

Informazioni sul regolamento sull'uso delle tecnologie a scuola

La ePolicy è un documento che deve essere condiviso con la comunità scolastica e a cui va data visibilità sul sito. Rispetto a tale punto si consiglia di rendere accessibile sul sito web dell'Istituto in forma autonoma il regolamento e non come allegato, per accrescere la possibilità che i genitori ne prendano visione. Se possibile si consiglia che gli/le studenti/esse e i loro esercenti responsabilità genitoriale ne prendano visione e possano firmare il documento. Può anche essere l'occasione per fornire informazioni sull'uso responsabile del web e per dare consigli sull'uso della Rete a casa.

Queste informazioni sulla sicurezza in Internet a scuola devono essere spiegate ai genitori con attenzione, in modo da non allarmarli. Deve essere loro chiaro che è fondamentale nel percorso di crescita l'accompagnamento da parte di adulti competenti anche rispetto al mondo online, con l'obiettivo di aiutarli a sviluppare le competenze digitali necessarie alla convivenza civile e al futuro lavorativo di ragazzi e ragazze. Troppo spesso oggi assistiamo a una sorta di autoformazione al digitale da parte di bambini/e, a volte addirittura in età prescolare.

Anche il personale scolastico avrà una copia del regolamento e dovrà sottoscriverla, consapevole che l'uso di Internet verrà monitorato e segnalato, e tutto il personale scolastico sarà coinvolto nello sviluppo delle linee guida del regolamento stesso. Saranno, inoltre, responsabili dell'applicazione delle istruzioni sull'uso sicuro di Internet.

Gli insegnanti, inoltre, saranno provvisti di informazioni concernenti i diritti d'autore.

La scuola deve chiedere ai genitori degli/lle studenti/esse minori di 16 anni di età il consenso all'uso di Internet per il loro figlio e per la pubblicazione dei suoi lavori e delle sue fotografie. Gli/Le studenti/esse che hanno un'età superiore a 16 anni (o maggiorenni), non hanno bisogno del consenso scritto dei genitori. In ogni caso, è suggerito che l'Istituto richieda il consenso genitoriale a tutti i minorenni.

Eventuali commenti o suggerimenti connessi al regolamento possono essere inviati al Dirigente Scolastico o al responsabile del gruppo di lavoro dell'ePolicy.

Contenuti dannosi e materiali non adatti

Se l'accesso a Internet è un diritto, esso deve anche essere adeguato all'età degli utenti.

Per questo la scuola deve prendere tutte le necessarie precauzioni per evitare l'accesso online da parte di studenti e studentesse, a materiali non adatti a loro all'interno della scuola. Questo può avvenire attraverso l'adozione di sistemi di filtraggio software e hardware o attraverso Internet provider che forniscono un servizio ad hoc. Le esigenze possono variare in base all'età degli studenti e delle studentesse ed è possibile differenziare l'accesso (come spesso avviene tra studenti e docenti), ma le indicazioni sono di permettere un utilizzo adeguato

delle risorse web per creare un ambiente sicuro, simile a quello “reale” e che permetta agli studenti, fin da piccoli, di affrontare il web con la guida degli insegnanti.

L’obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l’età e la maturità degli/lle studenti/esse.

Cloud computing e strumenti online

Il cloud computing può diventare lo strumento per abbattere i costi per le scuole, permettendo di accedere a una grande quantità di programmi attraverso Internet, senza bisogno di acquistare e installare programmi localmente. Questo può permettere anche un risparmio rispetto alla manutenzione, in quanto il software viene gestito sui server ed è costantemente aggiornato. La scuola dovrebbe quindi unicamente occuparsi di aggiornare il sistema operativo e il browser. Altri applicativi disponibili online riguardano foto e video editing, grafica e presentazioni multimediali. Per utilizzarli è sufficiente un browser; inoltre, i file salvati possono essere disponibili per l’accesso anche da casa per proseguire il lavoro iniziato in classe, sotto la guida dell’insegnante. Infine, non dipendono dalla piattaforma, per cui possono funzionare con Linux, Windows, Mac e Android. La scuola dovrebbe prevedere account personali per l’accesso ai computer e, in base all’età, un indirizzo mail per gli studenti, oltre che per gli insegnanti. Questo aspetto faciliterebbe le comunicazioni tra docenti e studenti, la gestione del cloud, ma tali informazioni si aggiungono alla già notevole quantità di dati trattati nelle attività scolastiche: informazioni sugli studenti e sulle loro famiglie, sui loro problemi sanitari o di disagio sociale, sulle abitudini alimentari. Per gli aspetti legati alla privacy di tali impostazioni si veda la lezione dedicata.

Rispetto all’uso del cloud o di strumenti di comunicazione online è opportuno che la scuola si doti di una netiquette (regole di comportamento che devono essere osservate dagli utenti di Internet), crasi delle parole network ed etiquette (“galateo della Rete”). Prendendo spunto dalla prima netiquette, quella del 1995 ormai universalmente riconosciuta, è possibile elaborarne una dell’Istituto con la collaborazione della componente studentesca. Oppure, come avviene in alcune scuole secondarie, ogni classe a inizio anno può predisporre una serie di regole e tra questa anche una netiquette di classe.

Si ricorda che in Italia, col recepimento del GDPR, l’età minima per l’accesso ai social network è di 14 anni, 13 con il consenso genitoriale per tutti i social statunitensi. La netiquette può essere elaborata comunque anche alle secondarie di primo grado e in caso di uso diffuso delle tecnologie in classe, anche alla primaria. Le regole valgono anche per i videogiochi online, a cui spesso i bambini accedono prima di avere uno smartphone.

Checklist per la cybersecurity

- **Mantenere separate le reti didattica e segreteria:** importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall.
- **Aggiornare periodicamente software e Sistema operativo:** garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- **Definire la programmazione di backup periodici:** cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline).
- **Garantire formazione adeguata allo staff, incluso il corpo docenti:** la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
- **Testare regolarmente le possibili vulnerabilità.**
- **Preparare piani di azione in risposta ai problemi più seri: è** importante non dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione.
- **Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo:** se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate.
- **Impostare il browser per l'eliminazione dei cookies alla chiusura:** in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione.
- **Definire una policy sulle password: le password devono essere forti:**
  - · Richiedere password complesse con almeno 8 caratteri con numeri, maiuscole e minuscole e caratteri speciali.
  - · Sensibilizzare rispetto al non uso di password facilmente identificabili (nomi dei figli, compleanni, etc.).
  - · Non memorizzare le password nei dispositivi scolastici.
  - · Non condividere le password con nessuno.
- **Minimizzare i privilegi amministrativi:** solo poche persone autorizzate dovrebbero avere privilegi amministrativi. Studenti e la maggior parte dei docenti possono accedere con account con permessi limitati.
- **Sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile):** deve riguardare chiunque abbia accesso alla Rete,

studenti/esse, docenti, amministrazione e segreteria, includere i dispositivi della scuola e quelli personali, anche in caso di BYOD.

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.

Gli strumenti di comunicazione online divengono, nell'era dei nativi digitali, ottimo ausilio alla cominicazione. Bisogna, però , farne buon uso.La scuola è l'agenzia educativa che promuove l'educazione a tutto tondo della comunità educante e anche nel campo del digitale ha un ruolo fondamentale.

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. Sono diversi, infatti, gli strumenti di comunicazione online che possono essere utilizzati a scuola, integrando quelli più tradizionali e che possono rendere lo scambio comunicativo maggiormente interattivo e orizzontale. La sfida, allora, è quella di conoscere al meglio tali strumenti, sfruttarne le potenzialità e come sempre prevenire eventuali rischi correlati ad un uso poco consapevole degli stessi.

Grazie all'uso delle tecnologie digitali, da una comunicazione uno a molti, si può passare ad una comunicazione che per definizione può essere molti a molti, multimediale, bidirezionale e interattiva. Ciò naturalmente può rappresentare un'opportunità significativa anche in termini di un maggiore coinvolgimento degli studenti o dei genitori, o alla possibilità di usare diversi linguaggi (scrittura, immagini, video etc.) ma in taluni casi può anche rivelarsi un problema non sempre facile da gestire. Si pensi, ad esempio, all'uso talvolta smodato e senza regole che docenti, ragazzi o genitori fanno dei gruppi whatsapp.

In questo paragrafo dell'ePolicy vi invitiamo, quindi, a riflettere su come le tecnologie possano facilitare e migliorare la comunicazione a scuola, su quali potrebbero essere gli strumenti di comunicazione online più utili per il vostro Istituto, e a partire da quali regole essi dovrebbero essere utilizzati.

Per guidarvi in questa riflessione è opportuno innanzitutto richiamare le

caratteristiche della comunicazione messa in atto attraverso le tecnologie digitali e l'uso della Rete (quella che comunemente viene definita la Computer mediated communication) e comprendere come essa si differenzi sostanzialmente dalla cosiddetta comunicazione face to face. Ciò, infatti, ha implicazioni molto importanti su come gli strumenti di comunicazione online dovrebbero essere utilizzati a scuola, sulle regole da elaborare per il loro uso, e sulle tipologie di comunicazione che si vogliono implementare attraverso di essi. Non tutte le forme di comunicazione, infatti, sono adatte a viaggiare online perché, come vedremo, talvolta, il fraintendimento è dietro l'angolo o la tentazione dell'essere always on (sempre connessi) può essere più forte e degenerare in inutile stress.

Le caratteristiche della comunicazione mediata dalle tecnologie

Quando ci relazioniamo attraverso l'uso di strumenti di comunicazione online, mettiamo in atto una modalità comunicativa che ha caratteristiche e logiche proprie. Ecco, allora, alcuni aspetti importanti da tenere in considerazione e di cui è importante essere consapevoli quando si fa uso delle TIC nelle comunicazioni a scuola.

Nella comunicazione mediata dalle tecnologie non condividiamo lo stesso spazio e lo stesso contesto comunicativo con i nostri interlocutori. Per questo, talvolta, può accadere che si forniscano cornici interpretative molto diverse ai messaggi e ai contenuti scambiati. Essa, inoltre, generalmente non ci permette di accedere ai cosiddetti segnali della comunicazione non verbale (tono della voce, espressione del volto, gesti del corpo, pause…etc.) e non siamo in grado di vedere ed ascoltare direttamente gli effetti della nostra comunicazione sull'interlocutore. Ciò comporta che difficilmente potremo adeguare il nostro comportamento a partire da tali segnali. Il cosiddetto feed-back non tangibile e l'impossibilità di accedere ai segnali non verbali del nostro interlocutore, così come la distanza e la separazione mediante lo schermo, ci rendono meno empatici e quindi meno attenti a emozioni e potenziali reazioni dell'altra persona. Inoltre, la comunicazione che viaggia online, generalmente, si avvale di messaggi scritti che possono essere memorizzati, diffusi e permangono nel tempo. È sempre bene tenerlo a mente.

D'altro canto, grazie agli strumenti di comunicazione online, come già in parte sottolineato, possiamo usufruire dell'interattività del mezzo, superare le barriere spazio-temporali, usare un linguaggio multimediale, ipertestuale e accattivante, promuovere la partecipazione e il coinvolgimento dei diversi attori in gioco nel processo educativo (dai ragazzi ai genitori).

Ma quali sono i possibili strumenti di comunicazione online che possono essere utilizzati a scuola?

A tale proposito è importante effettuare una distinzione preliminare fra comunicazione interna e comunicazione esterna. Diversi strumenti di comunicazione online possono essere utilizzati dalla scuola, sia per raggiungere

target esterni, al fine di valorizzare e promuovere le attività portate avanti dall'Istituto (rivolgendosi ad esempio a istituzioni, famiglie, studenti non ancora iscritti, associazioni etc.) sia per far circolare all'interno della scuola informazioni di servizio o contenuti importanti fra i diversi attori scolastici (docenti, studenti, genitori, collaboratori scolastici etc.).

Fra gli strumenti di comunicazione esterna, ad esempio, troviamo in primis il sito web della scuola, eventuali profili sui social network (si pensi a Facebook, Instagram, Linkedin, Twitter, Youtube), la newsletter, il blog, una web-radio o una web tv scolastica. Tali strumenti, naturalmente, possono essere utilizzati anche per fornire informazioni di servizio rivolte a studenti o genitori. Sarebbe opportuno che la comunicazione esterna online della scuola fosse coordinata e fosse progettata a partire da un piano di comunicazione in grado di trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che l'Istituto porta avanti e a partire dalla condivisione di regole ben precise su cosa comunicare e come comunicarlo. La comunicazione esterna dell'Istituto potrebbe essere progettata ed implementata anche con il supporto degli studenti che potrebbero produrre contenuti multimediali da diffondere attraverso i vari canali in uso (video, foto, post sui social, articoli per il sito o per il blog etc.).

Fra gli strumenti di comunicazione interna, invece, troviamo il registro elettronico con tutte le sue funzionalità, la classica e-mail, gli strumenti di messaggistica istantanea che però hanno sempre più funzionalità tipiche anche dei social network, whatsapp o telegram, i gruppi Facebook, o ulteriori applicativi e piattaforme di lavoro condiviso e collaborativo come wiki, google doc, classroom che possono essere ampiamente utilizzati anche per facilitare e rendere più partecipata la didattica e la comunicazione a scuola.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne, come avviene generalmente fra i docenti mediante ad esempio l'uso di gruppi whatsapp o telegram, è importante ricordare quello che si può definire "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare. È importante sottolineare però che per le chat informali fra colleghi, o fra docenti e genitori, non esiste una vera e propria regolamentazione, e per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, che si elaborino regole condivise sull'uso delle stesse. Fra queste, ad esempio, ve ne suggeriamo alcune:

- *Mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;*
- *Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi fraintendimenti);*

- *Evitare di affrontare in chat argomenti troppo complessi e controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);*
- *Evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;*
- *Non condividere file multimediali troppo pesanti;*
- *Evitare il più possibile di condividere foto di studenti in chat;*
- *Indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;*
- *Evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo.*

Quando si usano invece chat formali, create ad esempio dal Dirigente scolastico per veicolare messaggi, informazioni e aggiornamenti relativi all'attività scolastica, la regolamentazione è prevista dalla contrattazione di Istituto.

A titolo esemplificativo, sullo stesso tema vi forniamo questo interessante "Manifesto per un uso consapevole di whatsapp" (permalink immagine "Manifesto uso whatsapp") a cura del Comune e degli Istituti Comprensivi di Ancona.

Altro strumento ormai centrale a disposizione delle scuole per la gestione di assenze, presenze, valutazioni, prenotazioni di incontri e comunicazioni con le famiglie è il registro elettronico.

Il registro elettronico permette di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su:

- ***andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);***
- ***risultati scolastici (voti, documenti di valutazione);***
- ***udienze (prenotazioni colloqui individuali);***
- ***eventi (agenda eventi);***
- ***comunicazione varie (comunicazioni di classe, comunicazioni personali)***

L'Istituto Comprensivo utilizza il registro elettronico Argo come strumento di comunicazione con le famiglie, di gestione della didattica e trasparenza delle procedure di valutazione degli studenti.

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.

"Secondo una ricerca di Skuola.net, nelle classi smartphone e tablet sono già una realtà consolidata: nel 56% dei casi l'uso è didattico e controllato dai prof. (...) Più della metà dei ragazzi (56%) dice di usare già il cellulare durante le lezioni: in 1 caso su 10 sono tutti i professori a cercare di sfruttare gli smartphone per rendere le spiegazioni più coinvolgenti; il 47% di loro, invece, si deve accontentare solo di alcuni docenti che credono nelle potenzialità delle tecnologie digitali per l'accrescimento della cultura personale. A più di 1 ragazzo su 3 - il 36% - viene chiesto di accenderli per approfondire le spiegazioni; nel 13% dei casi per usare App durante lezioni e compiti in classe; la stessa percentuale (13%) lo sfrutta per prendere appunti e organizzare lo studio".

Questi dati confermano che la strumentazione tecnologica personale viene utilizzata come integrazione nella e della didattica da parte dei docenti come possibilità per poter avvicinare gli studenti e le studentesse alle discipline, alle lezioni e facilitare lo studio nella sua organizzazione complessiva.

Lo smartphone, nello specifico, insieme al tablet sembrano essere i dispositivi privilegiati, ma la stessa ricerca di Skuola.net sottolinea anche che ***"il 16% chatta con gli amici, il 13% controlla i social network, il 12% naviga su Internet, il 4% cerca le soluzioni ai compiti in classe, la stessa quota (4%) gioca".***

Riguardo, quindi, all'uso degli strumenti vi è ancora un dibattito divisivo che sembra riversarsi direttamente sui docenti. Sono questi, infatti, a dover considerare di volta in volta il possibile impiego delle TIC in classe.

Di seguito sono analizzate le disposizioni ministeriali e infine le strategie che sono state messe in atto in classe con consapevolezza e responsabilità anche alla luce del quadro normativo e di indirizzo di riferimento.

Nel DPR 24 giugno 1998, n. 249 "Regolamento recante lo Statuto delle studentesse e degli studenti della scuola secondaria" (in GU 29 luglio 1998, n. 175), all'art. 2 (sezione Diritti), punto 8 lettera e si sottolinea "la disponibilità di un'adeguata strumentazione tecnologica" di cui la scuola deve dotarsi per offrirla ai propri studenti e alle studentesse che, d'altra parte, "sono tenuti ad avere nei confronti del capo d'istituto, dei docenti, del personale tutto della scuola e dei loro compagni lo stesso rispetto, anche formale, che chiedono per se stessi" (Art. 3, punto 2 sezione Doveri).

Più specificatamente, è nel DECRETO DEL PRESIDENTE DELLA REPUBBLICA 21 Novembre 2007, n. 235 "Regolamento recante modifiche ed integrazioni al decreto del Presidente della Repubblica 24 giugno 1998, n. 249", concernente lo statuto delle studentesse e degli studenti della scuola secondaria, che si introduce il Patto educativo di corresponsabilità e giornata della scuola (Art. 3) che definisce, attribuendole, le responsabilità fra istituzione scolastica e famiglia. Oggi, il Patto va letto anche in riferimento all'educazione dei ragazzi e delle ragazze all'uso dei nuovi dispositivi tecnologici, inclusi tablet e smartphone sia a scuola che a casa.

All'interno di tale cornice normativa, si inserisce la circolare n° 362 del 25 agosto 1998 "Uso del telefono cellulare nelle scuole" che ha come oggetto particolare l'uso del cellulare a scuola da parte dei docenti anche durante le ore di lezione. La circolare contiene tali orientamenti: "è chiaro che tali comportamenti - laddove si verifichino - non possono essere consentiti in quanto si traducono in una mancanza di rispetto nei confronti degli alunni e recano un obiettivo elemento di disturbo al corretto svolgimento delle ore di lezione che, per legge, devono essere dedicate interamente all'attività di insegnamento e non possono essere utilizzate - sia pure parzialmente - per attività personali dei docenti". Un orientamento, dunque, volto a punire l'uso personale del dispositivo solo per il corpo docente.

La DM n. 30 del 15/03/2007 "Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, doveri di vigilanza e di corresponsabilità dei genitori e dei docenti", invece, si concentra su più elementi che interessano, questa volta, anche gli studenti e le studentesse in un'ottica non punitiva ma risarcitoria e riparatoria.

In prima battuta, si ribadiscono alcuni doveri contenuti nell'articolo 3 del D.P.R. n. 249/1998: "per ciascuno studente, di non utilizzare il telefono cellulare, o altri dispositivi elettronici, durante lo svolgimento delle attività didattiche, considerato che il discente ha il dovere:

- di assolvere assiduamente agli impegni di studio anche durante gli orari di

lezione (comma 1);

- di tenere comportamenti rispettosi degli altri (comma 2), nonché corretti e coerenti con i principi di cui all'art. 1 (comma 3);
- di osservare le disposizioni organizzative dettate dai regolamenti di istituto (comma 4)" (DM n. 30 del 15/03/2007 - "Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, doveri di vigilanza e di corresponsabilità dei genitori e dei docenti").

Come stabilito dall'autonomia scolastica, è nei singoli regolamenti d'Istituto che si inseriscono le sanzioni disciplinari in caso di uso scorretto dei cellulari da parte dei ragazzi e delle ragazze in classe.

In seconda battuta, si sottolinea l'importanza del Patto educativo di corresponsabilità condividendo diritti e doveri fra scuola e famiglia la quale deve impegnarsi "a rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone o alle strutture scolastiche o, più in generale, violino i doveri sanciti dal regolamento di istituto e subiscano, di conseguenza, l'applicazione di una sanzione anche di carattere pecuniario".

Resta la responsabilità deontologica e professionale dei dirigenti, dei docenti e del personale ATA che hanno il dovere di vigilare sui comportamenti degli studenti e delle studentesse il quale sussiste in tutti gli spazi scolastici e di segnalare eventuali infrazioni suscettibili di sanzioni disciplinari.

Con la DM n. 104 del 30/11/2007 "Linee di indirizzo e chiarimenti sulla normativa vigente sull'uso di telefoni cellulari e di altri dispositivi elettronici nelle comunità scolastiche" si chiarisce, anche in virtù della normativa allora vigente posta a tutela della privacy, il divieto di utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali. In altre parole, è punibile sia a livello civile che penale (oltre che le sanzioni previste dagli artt. 3 e 4, d.P.R. 24 giugno 1998, n. 249 - "Regolamento recante lo statuto delle studentesse e degli studenti della scuola secondaria"), chi abusa dei dati personali altrui raccolti (immagini, filmati, registrazioni vocali…).

E proprio riguardo il Codice della Privacy, Digs. 196/2003, modificato e integrato dal D. Lgs. 101/2018 recependo il regolamento UE 2016/679 e art.10 del Codice Civile, è necessario considerare che "l'uso di cellulari e smartphone è in genere consentito per fini strettamente personali, ad esempio per registrare le lezioni, e sempre nel rispetto delle persone. Spetta comunque agli istituti scolastici decidere nella loro autonomia come regolamentare o se vietare del tutto l'uso dei cellulari. Non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. È bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente

in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati. Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line".

La riproduzione dei dati deve, pertanto, rispondere alla sola esigenza di documentazione dell'attività didattica previa informativa e autorizzazione firmata o esplicito consenso (sono comprese le recite, i saggi scolastici e le gite raccolte dai genitori che non si configurano come violazione della privacy se raccolti per fini personali, familiari e non vengono pubblicate on line, in particolare sui social network).

A tal proposito, è bene ricordare la Legge n. 71 del 2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che ancor di più cerca di contrastare manifestazioni comportamentali di soggetti minorenni a danno di altri minorenni che pongono "in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo" attraverso le tecnologie digitali. Dove anche gli adulti tutti, docenti e genitori, hanno responsabilità specifiche oltre che un ruolo di vigilanza e di educazione dei minori stessi.

Le disposizioni che si sono adottate in passato hanno perciò chiuso ad ogni possibilità di utilizzo misto dei dispositivi personali nelle attività didattiche come strumenti di socialità positiva e di occasione per l'educazione alle tecnologie digitali.

La questione qui descritta è stata affrontata, per la prima volta in maniera integrata, nel Piano Nazionale Scuola Digitale emanato dal Miur con la Legge 107 del 2015: "al fine di sviluppare e di migliorare le competenze digitali degli studenti e di rendere la tecnologia digitale uno strumento didattico di costruzione delle competenze in generale, il Ministero dell'istruzione, dell'università e della ricerca adotta il Piano nazionale per la scuola digitale (...)".

L'attenzione verso le tecnologie digitali e il loro utilizzo in classe diventa così inclusivo e creativo, nel senso che le stesse vengono riproposte come strumenti da inserire nella didattica e nelle sperimentazioni laboratoriali. L'uso viene consentito per scopi prettamente didattici, sotto il controllo e la responsabilità del docente che pianifica l'attività didattica.

BYOD letteralmente significa "porta il tuo dispositivo" ed è un'espressione che descrive quelle politiche aziendali che in tutto il mondo consentono agli impiegati di utilizzare i propri dispositivi personali in ambiente di lavoro.

In tal senso, gli smartphone, i tablet e i pc personali possono essere integrati nel lavoro nelle classi quando ben progettato e calibrato per discipline e obiettivi formativi e didattici: si pensi, a titolo di esempio, agli student response systems ossia alla possibilità degli studenti e delle studentesse di rispondere a quiz e

sondaggi utilizzando direttamente il proprio smartphone come telecomando sempre sotto la guida e il controllo dell'insegnante.

A tale scopo, il MIUR, in collaborazione con AGID (l'Agenzia per il Digitale) e il Garante per la Privacy, ha elaborato apposite linee guida per promuovere il **3.4. Strumentazione personale** Si tratta di un vero e proprio decalogo che apre alla didattica integrata tramite un uso dei propri dispositivi personali in classe e alla sicurezza delle interazioni e delle relazioni fra pari tramite le tecnologie digitali.

Di seguito, i dieci i punti del Miur per l'uso dei dispositivi mobili a scuola, BYOD (Bring your own device):

- **Ogni novità comporta cambiamenti.** Ogni cambiamento deve servire per migliorare l'apprendimento e il benessere delle studentesse e degli studenti e più in generale dell'intera comunità scolastica
- **I cambiamenti non vanno rifiutati, ma compresi e utilizzati per il raggiungimento dei propri scopi.** Bisogna insegnare a usare bene e integrare nella didattica quotidiana i dispositivi, anche attraverso una loro regolamentazione. Proibire l'uso dei dispositivi a scuola non è la soluzione. A questo proposito ogni scuola adotta una Politica di Uso Accettabile (PUA) delle tecnologie digitali.
- **La scuola promuove le condizioni strutturali per l'uso delle tecnologie digitali.** Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile dei dispositivi personali (BYOD). Le tecnologie digitali sono uno dei modi per sostenere il rinnovamento della scuola.
- **La scuola accoglie e promuove lo sviluppo del digitale nella didattica.** La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica. Dirigenti e insegnanti attivi in questi campi sono il motore dell'innovazione. Occorre coinvolgere l'intera comunità scolastica anche attraverso la formazione e lo sviluppo professionale.
- **I dispositivi devono essere un mezzo, non un fine.** È la didattica che guida l'uso competente e responsabile dei dispositivi. Non basta sviluppare le abilità tecniche, ma occorre sostenere lo sviluppo di una capacità critica e creativa.
- **L'uso dei dispositivi promuove l'autonomia delle studentesse e degli studenti.** È in atto una graduale transizione verso situazioni di apprendimento che valorizzano lo spirito d'iniziativa e la responsabilità di studentesse e gli studenti. Bisogna sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione, anche in vista di un apprendimento lungo tutto l'arco della vita.

- **Il digitale nella didattica è una scelta: sta ai docenti introdurla e condurla in classe.** L'uso dei dispositivi in aula, siano essi analogici o digitali, è promosso dai docenti, nei modi e nei tempi che ritengono più opportuni.
- **Il digitale trasforma gli ambienti di apprendimento.** Le possibilità di apprendere sono ampliate, sia per la frequentazione di ambienti digitali e condivisi, sia per l'accesso alle informazioni, e grazie alla connessione continua con la classe. Occorre regolamentare le modalità e i tempi dell'uso e del non uso, anche per imparare a riconoscere e a mantenere separate le dimensioni del privato e del pubblico.
- **Rafforzare la comunità scolastica e l'alleanza educativa con le famiglie.** È necessario che l'alleanza educativa tra scuola e famiglia si estenda alle questioni relative all'uso dei dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione. Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.
- **Educare alla cittadinanza digitale è un dovere per la scuola.** Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

Anche il progetto Generazioni Connesse, d'altra parte, va verso la responsabilizzazione di tutti i soggetti in gioco nel processo educativo e didattico dove l'utilizzo delle tecnologie e dei dispositivi anche personali va mediato e calibrato sviluppando un pensiero critico.

L'ePolicy, documento di indirizzo e programmazione interno al progetto e insieme ai regolamenti previsti (che pure andrebbero integrati), viene redatto per identificare tali aspetti in termini di utilizzo del proprio smartphone a scuola e in classe, richiamando anche l'azione #15 del PNSD (Scenari innovativi per lo sviluppo di competenze digitali applicate) nell'ottica di potenziare le competenze di cittadinanza digitale.

In tale ottica, occorre integrare i Regolamenti già esistenti per disciplinare l'utilizzo delle TIC all'interno della scuola (es. la dotazione di filtri), prevedere misure per prevenire diverse tipologie di rischio (non solo quelle più frequenti come il cyberbullismo) e stabilire procedure specifiche per rilevare e gestire le diverse problematiche.

Il nostro piano d'azioni

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

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
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte delpersonale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personal

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

Scegliere almeno 1 di queste azioni:

- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali1
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Nel nostro istituto è stato predisposto un programma di interventi di sensibilizzazione eprevenzione diretti all'itero gruppo alunni/genitori/docenti. L'intenzione è di affrontare problematiche ad ampio raggio che consentano l'individuazione di rischi specifici di un gruppo o di singoli alunni, per i quali potrebbe essere necessario un intervento selettivo o personalizzato. Si tratta dunque, di interventi di sensibilizzazione alle principali tematiche trattatate e di formazione specifica sui rischi e le problematiche legate alla diffusione delle tecnologie dogitale e dell'accesso alla rete e delle tecnologie dell'informazione e comunicazione.

I rischi online rappresentano tutte quelle situazioni problematiche derivanti da un uso non consapevole e non responsabile delle tecnologie digitali da parte di bambini/e, ragazzi e ragazze: adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia (recenti ricerche hanno sottolineato come la maggior parte degli adolescenti reperisca in Rete informazioni inerenti la sessualità, col rischio, spesso effettivo, del diffondersi di informazioni scorrette e/o l'avvalorarsi di falsi miti), pedopornografia (con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone minorenni), gioco d'azzardo o gambling, internet addiction, videogiochi online (alcuni rischi associati possono essere ad esempio: contatti impropri con adulti, contenuti violenti e/o inadeguati; acquisti incontrollati, etc.), esposizione a contenuti dannosi o inadeguati (es. contenuti razzisti, che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, etc.), etc.

Per far sì che un intervento di sensibilizzazione sia efficace, è quindi importante fornire ai beneficiari informazioni chiare su quello che è lo stato attuale del tema che vogliamo trattare (ad es. se si vuol trattare il tema del Cyberbullismo, sarà opportuno fornire informazioni su quali sono le caratteristiche del fenomeno e i dati rappresentativi). In questo modo gli utenti avranno tutte le informazioni necessarie per avere una fotografia chiara del contenuto che stiamo trattando e del perché è necessario impegnarsi verso un cambiamento (motivazione al cambiamento).

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

- spingere le persone a desiderare un cambiamento;
- porre in evidenza la possibilità di generare un cambiamento;
- individuare le azioni che consentono di produrre il cambiamento.

Un'attività di sensibilizzazione dovrebbe quindi fornire non solo le informazioni necessarie, ma anche illustrare le possibili soluzioni o comportamenti da adottare.

Interventi di prevenzione

Il concetto di prevenzione nasce in ambito epidemiologico e seguendo quanto riportato dal Ministero della Salute si può sintetizzare come un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere e conservare lo stato di salute ed evitare l'insorgenza di malattie.

Parlando di prevenzione in ambito digitale si potrebbe tradurre quanto appena detto con 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.

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

La letteratura storicamente distingue tre livelli di prevenzione: primaria, secondaria e terziaria (Caplan, G. (1964). Principles of preventive psychiatry. New York: Basic Books), nel dibattito comune questa classificazione è presente ancora oggi, ma la comunità scientifica internazionale non è concorde e si preferisce utilizzare la classificazione proposta dall'Institute of Medicine che distingue i tre livelli in:

- **Prevenzione Universale.** Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale. Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che "trattano" un gruppo con un problema specifico. Tuttavia, questi interventi possono produrre cambiamenti in grandi popolazioni (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale).
- **Prevenzione Selettiva.** Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti.
- **Prevenzione Indicata**. Un programma di intervento sul caso specifico, è quindi pensato e strutturato per adattarsi agli/lle studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/lla ragazzo/a.

Fonte: Muñoz, R. F., Mrazek, P. J., & Haggerty, R. J. (1996). Institute of Medicine report on prevention of mental disorders: Summary and commentary. American Psychologist, 51(11), (1116–1122).

Il modello diviso in tre livelli può essere un'utile guida per affrontare e prevenire ogni possibile situazione di disagio, è tuttavia comprensibile la difficoltà di poter strutturare soluzioni ed interventi multilivello da parte dell'Istituzione Scolastica senza sicuramente consigliati proprio perchè vanno a formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i/le ragazzi/e sperimentano online.

Come sappiamo, le dimensioni che il fenomeno coinvolge sono molteplici e non puramente tecniche e si rifanno alla capacità dei più giovani di gestire situazioni complesse che richiedono: la capacità di gestire la relazione con l'altro/a diverso/a da sé, le dimensioni dell'affettività e della sessualità, il riconoscimento di un limite, anche, ma non solo, legato ad una dimensione di legalità, l'utilizzo sicuro e consapevole delle tecnologie digitali.

Per questo motivo la scuola deve rafforzare la sua capacità di rispondere anche a questi bisogni attraverso strumenti e misure specifiche. Allo stesso modo quando un evento problematico connesso ai rischi online coinvolge il contesto scolastico, è fondamentale per la scuola poter dare una risposta il più possibile integrata, che trovi la sua espressione di indirizzo in procedure chiare di cui deve dotarsi e che includano la collaborazione (prevedendo accordi specifici) con la rete dei servizi locali (in primis le ASL e la Polizia Postale).

Inoltre, la responsabilità dell'azione preventiva ed educativa chiama in campo diverse agenzie educative oltre alla scuola, come la famiglia, ma non solo (istituzioni, associazioni, società civile, etc.), ciascuna con un proprio compito nei confronti di bambini e bambine e di adolescenti. Tali agenzie sono chiamate a collaborare ad un progetto comune, nell'ambito di funzioni educative condivise. La necessità di questa collaborazione nasce, più o meno consapevolmente, dal riconoscimento sia da parte dei genitori che da parte degli insegnanti della rispettiva difficoltà a svolgere da soli la propria funzione formativa ed educativa. E questo, anche a causa della sproporzione tra le competenze sempre crescenti che le tecnologie digitali richiedono loro e quelle che si avvertono di possedere. La necessità di supportare un uso positivo e consapevole delle TIC da parte dei più giovani, sia in un'ottica di tutela dai rischi potenziali che nella valorizzazione delle opportunità esistenti, pone la scuola e i genitori di fronte alla sfida di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente.

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).

Nel bullismo tradizionale, solitamente, la vittima che viene presa di mira è percepita come più debole e incapace di difendersi.

Il più forte, quindi, assume atteggiamenti prevaricatori nei confronti del più debole, a partire da una certa "asimmetria di potere".

Ciò, naturalmente, può accadere anche nel caso del cyberbullismo. Mentre nel bullismo tradizionale, però, il potere presenta connotati ben precisi, potrebbe essere, ad esempio, di tipo fisico (legato alla forza o alla statura) o sociale (legato alla popolarità), il potere online può derivare semplicemente dal possesso di specifiche competenze o di alcuni contenuti (immagini, video, confessioni) che potrebbero essere utilizzati per danneggiare la vittima.

Solitamente, quando si parla di cyberbullismo o di bullismo è necessario che

vittima e bullo/cyberbullo siano minori o comunque adolescenti (sono esclusi, quindi, dalla definizione episodi di prevaricazione che avvengono fra adulti o fra un adulto e un minore).

Un'altra definizione di cyberbullismo è quella che ci fornisce la Legge Ferrara, ovvero la l. 71/2017 " Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo"(che affronteremo in modo più approfondito più avanti). Il testo 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 online 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" (Art. 1- Comma 2).

Le caratteristiche del fenomeno

Ma quali sono le caratteristiche specifiche del cyberbullismo rispetto al bullismo cosiddetto tradizionale? Come sottolinea la Willard i tratti specifici del bullismo online sono correlati all'impatto che le tecnologie digitali hanno nella vita dei ragazzi (e di tutti noi) e alle caratteristiche stesse della Rete (Willard, N. (2005), *Educator's guide to cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress, Research Press, Illinois). Vediamole a seguire:*

- **L'impatto:** la diffusione di materiale tramite Internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online e continuare a diffondersi). Un contenuto offensivo e denigratorio online può, quindi, diventare virale e distruggere in alcuni casi la reputazione della vittima. Nelle situazioni più gravi, le vittime di cyberbullismo si trovano costrette a dover cambiare scuola o addirittura città, ma questo spesso non le aiuta. La Rete, si sa, è ovunque.
- **La convinzione dell'anonimato:** chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. Sentendosi protetti dall'anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. È importante tenere bene a mente, però, che quello dell'anonimato è un "falso mito della Rete". Ogni nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale. L'anonimato del

cyberbullo, inoltre, è anche uno dei fattori che stanno alla base del forte stress percepito dalla vittima, la quale molte volte non può dare né un nome e né un volto al proprio aggressore;

- **L'assenza di confini spaziali:** il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio. La vittima può essere raggiungibile anche a casa e vive nella costante percezione di non avere vie di fuga. Spegnere il cellulare o il computer non basta, così come cancellare tutti i propri profili social. Il solo pensiero che eventuali contenuti denigratori continuino a diffondersi online è doloroso e si accompagna ad un senso costante di rabbia e impotenza.
- **L'assenza di limiti temporali:** può avvenire a ogni ora del giorno e della notte.
- **L'indebolimento dell'empatia:** esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simile a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Tale sensazione è data dall'attivazione di una particolare area del cervello. Quando le interazioni avvengono prevalentemente online la funzione speciale di questi neuroni viene meno (mancando la presenza fondamentale dell'altro che è sostituito dal dispositivo). La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.
- **Il feedback non tangibile:** il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

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

Per questo il fenomeno viene talvolta sottovalutato anche dal mondo adulto, familiare e scolastico.

La mediazione tecnologica, infatti, porta ad un certo distanziamento fra aggressore e vittima, causando quello che Bandura ha definito come "disimpegno morale". Si tratta di un indebolimento del controllo morale interno dell'individuo, con la conseguente minimizzazione delle responsabilità individuali. Tale fenomeno vale non solo per il cyberbullo, ma anche per i cosiddetti bystander, ossia coloro che sono spettatori dei fatti.

A ciò si aggiungono altre convinzioni o tendenze frequenti nell'uso della Rete sia da parte dei giovani che degli adulti:

- Percezione che online non ci siano norme sociali da rispettare: fra i giovani spesso vige la falsa convinzione secondo cui la Rete sia uno spazio virtuale lontano dalla realtà, in cui vige libertà assoluta e in cui regole e norme sociali della vita quotidiana non valgono;
- La sperimentazione online di identità e personalità multiple: la Rete è per i minori il luogo virtuale per eccellenza in cui mettersi in gioco "fingendo di essere ciò che non si è" per il semplice gusto di sperimentare nuove forme di identità e comportamento;
- Il contesto virtuale come un luogo di simulazione e giochi di ruolo: "la vita sullo schermo" e tutti i comportamenti messi in atto online vengono percepiti solo come un gioco.
- Diffusione di responsabilità: tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili delle azioni del cyberbullo facendo accrescere la portata dell'azione; mettere un "like" su un social network commentare o condividere una foto o un video che prende di mira qualcuno o semplicemente tacere pur sapendo, mette ragazzi e ragazze nella condizione di avere una responsabilità.

Ma d'altro canto sono proprio loro che possono "fare la differenza" perché la responsabilità è condivisa: il gruppo "silente" che partecipa senza assumersi la responsabilità, rappresenta, in realtà, anche l'elemento che può fermare una situazione di cyberbullismo. E questo appunto costituisce un gancio educativo.

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

- **cyberbullismo diretto:** il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei.
- **cyberbullismo indiretto:** il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

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

Nel nostro Istituto, per arginare i casi di cyberbullismo, si è istituita la figura del Referente che, attraverso interventi di sensibilizzazione del corpo docente e

partecipazione a corsi di aggiornamento, informa, sensibilizza e previene tali fenomeni.

Come riconoscere casi di cyberbullismo?

Di seguito, alcuni segnali generali che può manifestare la potenziale vittima di cyberbullismo:

- *Appare nervosa quando riceve un messaggio o una notifica;*
- *Sembra a disagio nell'andare a scuola o finge diessere malata (ha spesso mal di stomaco o mal di testa);*
- *Cambia comportamento ed atteggiamento in modo repentino;*
- *Mostra ritrosia nel dare informazioni su ciò che fa online;*
- *Soprattutto dopo essere stata online, mostra rabbia o si sente depressa;*
- *Inizia ad utilizzare sempre meno Pc e telefono (arrivando ad evitarli);*
- *Perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;*
- *Il suo rendimento scolastico peggiora.*

La normativa in materia

Il Parlamento italiano ha approvato il 18 maggio 2017 la Legge 71/2017, "Disposizioni a tutela dei minoriper la tutela e la prevenzione ed il contrasto del fenomeno del cyberbullismo", una legge a tutela dei minori per la prevenzione e il contrasto al cyberbullismo che prevede misure prevalentemente a carattere educativo/rieducativo. La legge pone al centro il ruolo dell'istituzione scolastica nella prevenzione e nella gestione del fenomeno e ogni Istituto scolastico dovrà provvedere ad individuare fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo.

La L.71/17 introduce per la prima volta nell'ordinamento giuridico anche una definizione di cyberbullismo (come già riportato sopra).

Nella consapevolezza che le azioni efficaci siano quelle che ricorrono agli strumenti educativi, rieducativi e di mediazione del conflitto, esistono tuttavia responsabilità da conoscere, la possibilità di commettere reati o danni civili e specifici dispositivi giuridici.

Sempre la Legge 71/2017 introduce un provvedimento di carattere amministrativo per gli autori di atti di cyberbullismo, la procedura di

ammonimento da parte del Questore: il minore autore può essere convocato dal Questore e ammonito se ritenuto responsabile delle azioni telematiche.

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

Chi compie atti di bullismo e cyberbullismo può anche essere responsabile di reati penali e danni civili.

I ragazzi e le ragazze che fanno azioni di bullismo possono commettere reati. Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

- ***percosse (art. 581),***
- ***lesione personale (art. 582),***
- ***ingiuria (art. 594),***
- ***diffamazione (art. 595),***
- ***violenza privata (art. 610),***
- ***minaccia (art. 612),***
- ***danneggiamento (art. 635).***

Nei casi più gravi, basta la denuncia ad un organo di polizia o all'autorità giudiziaria per attivare un procedimento penale (per es. lesioni gravi, minaccia grave, molestie); negli altri casi, la denuncia deve contenere la richiesta che si proceda penalmente contro l'autore di reato (querela).

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

Per il nostro ordinamento l'imputabilità penale (ossia la responsabilità personale per i reati commessi) scatta al quattordicesimo anno. La legge sancisce che "nessuno può essere punito per un fatto preveduto dalla legge come reato, se al momento in cui l'ha commesso, non era imputabile". Cosa si intende per "imputabilità"? Vuol dire avere la cosiddetta "capacità d'intendere e volere".

Dunque, per poter avviare un procedimento penale nei confronti di un

minore è necessario:

- che abbia almeno compiuto 14 anni;
- che, comunque, anche se maggiore di 14 anni, fosse cosciente e volente al momento del comportamento, cioè in grado di intendere e volere (tale non sarebbe, per esempio, un ragazzo con degli handicap psichici).

L'atto di bullismo può violare sia la legge penale, sia quella civile, quindi può dar vita a due processi, l'uno penale e l'altro civile.

Le responsabilità per atti di bullismo e cyberbullismo compiute dal minorenne possono ricadere anche su:

- i genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando).
- gli insegnanti e la scuola: perché nei periodi in cui il minore viene affidato all'Istituzione scolastica il docente è responsabile della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa. A pagare in primis sarà la scuola, che poi potrà rivalersi sul singolo insegnante. La responsabilità si estende anche a viaggi, gite scolastiche, manifestazioni sportive organizzate dalla scuola (culpa in vigilando).
- esiste poi una culpa in organizzando, che si ha quando la scuola non mette in atto le azioni previste per la prevenzione del fenomeno o per affrontarlo al meglio (così come previsto anche dalla normativa vigente).

Responsabilità dei genitori

Se il minore non ha compiuto i 14 anni, non risponde penalmente per l'evento, ma i genitori saranno tenuti al risarcimento del danno, per presunta "culpa in educando", così come previsto dal codice civile per i fatti commessi dal figlio. Non c'è responsabilità penale dei genitori, perché la responsabilità penale è personale.

Se i genitori riescono a fornire la prova di aver fatto di tutto per impedire il fatto, possono essere **esonerati dall'obbligo di risarcire il danno causato dal figlio**. Ma questo tipo di prova è molto difficile da produrre, perché significa poter dare evidenza certa:

- *di aver educato e istruito adeguatamente il figlio (valutazione che viene dal giudice commisurata alle circostanze, ovvero tra l'altro alle condizioni economiche della famiglia e all'ambiente sociale a cui appartiene),*

- *di aver vigilato attentamente e costantemente sulla sua condotta,*
- *di non aver in alcun modo potuto impedire il fatto, stante l'imprevedibilità e repentinità, in concreto, dell'azione dannosa.*

Responsabilità degli insegnanti

Cosa succede nel caso di comportamenti penalmente rilevanti o di danni procurati ad esempio a scuola, durante una gita scolastica?

In questi casi interviene l'art. 2048 del Codice Civile (responsabilità dei precettori) e l'art. 61 della L. 312/1980 n. 312 (responsabilità patrimoniale del personale direttivo, docente educativo e non docente). In base a queste norme, quindi, gli insegnanti sono responsabili dei danni causati a terzi "dal fatto illecito dei loro allievi… nel tempo in cui sono sotto la loro vigilanza".

Se si tratta di una scuola pubblica, la responsabilità si estende alla pubblica amministrazione, che si surroga al suo personale nelle responsabilità civili derivanti da azioni giudiziarie promosse da terzi. Se si tratta di una scuola privata, sarà la proprietà dell'Istituto a risponderne. Gli insegnanti potranno essere chiamati a rispondere personalmente solo in caso di azione di rivalsa per dolo o colpa grave, da parte dell'amministrazione. L'insegnante ha un dovere di vigilanza e di conseguenza viene addebitata, in caso di comportamento illecito del minore affidato, una colpa presunta, cioè una "culpa in vigilando", come inadempimento dell'obbligo di sorveglianza sugli allievi. Di questa colpa/responsabilità si può essere liberati dimostrando di non aver potuto impedire il fatto. Si tiene conto in questi casi dell'età e del grado di maturità dei ragazzi, della concreta situazione ambientale, etc.

Inoltre, l'insegnante deve dimostrare di aver adottato in via preventiva le misure idonee ad evitare la situazione di pericolo.

Ma in quali momenti l'insegnante è responsabile?

Va considerato tutto il tempo dell'affidamento dell'alunno alla scuola. Quindi, non soltanto le ore delle attività didattiche, ma anche tutti gli altri momenti della vita scolastica, compresa la ricreazione, la pausa pranzo, la palestra, le uscite e i viaggi di istruzione etc.

Come intervenire?

La Legge 71/2017 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).
- Salvo che il fatto costituisca reato, il Dirigente Scolastico qualora venga a conoscenza di atti di cyberbullismo deve informare tempestivamente i genitori dei minori coinvolti (art.5).

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

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

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

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

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

Cos'è l'hate speech?

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti…) 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, etc.) ai danni di una persona o di un gruppo.

"L'incitamento all'odio deve essere inteso, quindi, come comprensivo di tutte le forme di espressione che diffondono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o altre forme di odio generate dall'intolleranza, ivi comprese: l'intolleranza espressa dal nazionalismo, e dall'etnocentrismo aggressivi, la discriminazione e l'ostilità nei confronti delle minoranze, dei migranti e delle persone con origine straniera" (www.coe.int). Tale fenomeno, purtroppo, negli ultimi anni si è fortemente diffuso e rafforzato soprattutto attraverso l'uso della Rete, i social network in particolar modo, dove non è difficile e infrequente trovare forme di odio e hate speech online particolarmente violente. Per questo è estremamente importante affrontarlo con ragazze e ragazzi anche a scuola.

In questo paragrafo dell'ePolicy vi invitiamo a riflettere su questa problematica e a descrivere nel documento in che modo il vostro Istituto intende prevenire ed affrontarla. Proviamo, quindi, a conoscere meglio il fenomeno.

Come riconoscerlo e prevenirlo

Scopriamo insieme le caratteristiche dell'hate speech, come riconoscerlo e prevenirlo, a partire dal documento No hate ita (che vi invitiamo a leggere integralmente per un ulteriore approfondimento):

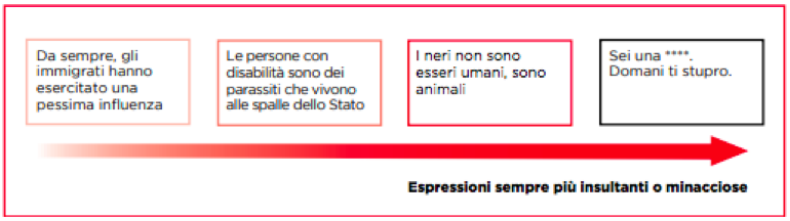
- **Il discorso d'odio procura sofferenza.** La parola ferisce, e a maggior ragione l'odio! Il discorso può violare i diritti umani. Il discorso d'odio online non è meno grave della sua espressione offline, ma è più difficile da individuare e da combattere.
- **Gli atteggiamenti alimentano gli atti.** Il discorso dell'odio è pericoloso anche perché può condurre a più gravi violazioni dei diritti umani, e perfino alla violenza fisica. Può contribuire a inasprire le tensioni razziali e altre forme di discriminazione e di violenza.
- **L'odio online non è solo espresso a parole.** Internet ci permette di comunicare rapidamente e in modi svariati, ad esempio, mediante i social media e i giochi online, molto spesso, d'altronde, in maniera anonima. L'odio online può esprimersi sotto forma di video e foto, come pure, più solitamente, di contenuto testuale. Le forme visive o multimediali hanno sovente un impatto più forte sugli atteggiamenti (consci e inconsci).
- **L'odio prende di mira sia gli individui che i gruppi.** L'odio online può prendere di mira dei gruppi che spesso sono già vulnerabili sotto altri aspetti, come i richiedenti asilo, le minoranze religiose o le persone con disabilità. Tuttavia, anche i singoli individui sono sempre maggiormente oggetto di attacchi. Le conseguenze sono talvolta fatali, come dimostrato da numerosi fatti di cronaca riferiti dai media, riguardanti giovani vittime di cyberbullismo che sono state spinte al suicidio.
- **Internet è difficilmente controllabile.** La diffusione di messaggi di incitamento all'odio è maggiormente tollerata su Internet rispetto al mondo offline ed è sottoposta a minori controlli. È ugualmente più facile (e comporta meno rischi) insultare o molestare online, perché le persone spesso si esprimono sotto la copertura dell'anonimato.
- **Ha radici profonde.** Gli atteggiamenti e le tensioni sociali che suscitano sentimenti di odio online affondano le loro radici nella società, e non sono diversi, in genere, da quelli che alimentano il discorso dell'odio offline.
- **Impunità e anonimato.** Sono le due presunte caratteristiche delle interazioni sociali in rete: l'impunità e l'anonimato. Queste abbassano le remore etiche. In realtà, però, qualsiasi azione compiuta sul web consente di rintracciare il suo autore.

Come riconoscerlo?

Il discorso dell'odio si manifesta con un ampio spettro di azioni: sebbene tutte le espressioni che istigano all'odio meritino di essere classificate come malvagie, ne esistono alcune che possono essere peggiori di altre. È utile, quindi, prendere in considerazione alcuni aspetti:

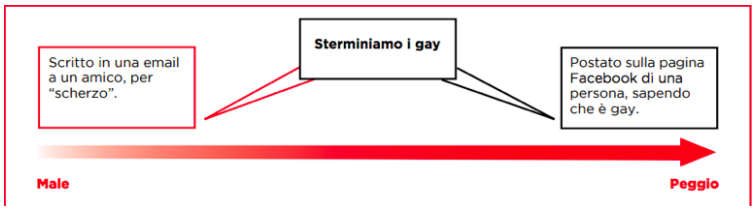
Il contenuto e il tono

Certe espressioni di odio sono più estreme, utilizzano termini più insultanti e possono perfino istigare altri ad agire. All'altra estremità della scala, troviamo insulti più moderati o generalizzazioni eccessive, che presentano certi gruppi o individui sotto una cattiva (e perfino sotto falsa) luce.



L'intenzione degli autori degli insulti

Ci può capitare di offendere gli altri senza volerlo, e poi di pentircene, e perfino di ritirare quanto abbiamo detto. Nei due esempi seguenti, entrambe le affermazioni sono intolleranti e sgradevoli, ma una è stata scritta con l'intenzione di offendere e fare del male.

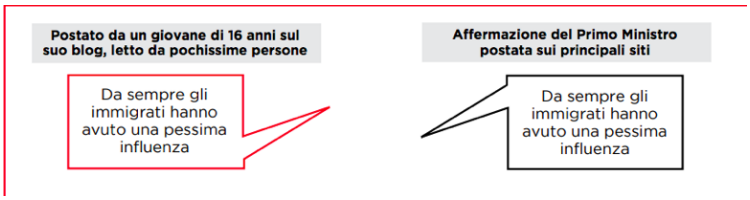


I bersagli o i bersagli potenziali

Alcuni gruppi, o individui, possono essere più vulnerabili di altri alle critiche. Può dipendere dal modo in cui sono globalmente considerati nella società, o da come sono rappresentati nei media, oppure dalla loro situazione personale, che non permette loro di difendersi efficacemente. L'esempio qui sotto mostra come la stessa espressione, applicata a gruppi diversi, possa avere un impatto molto diverso. Quella di destra rischia di essere molto più pregiudizievole.

Il contesto

Il contesto di una particolare espressione di odio è legato talvolta a circostanze storiche e culturali specifiche. Può includere altri fattori, come il mezzo utilizzato e il gruppo preso di mira, le tensioni o i pregiudizi esistenti, l'autorità del suo autore, etc.



L'impatto o l'impatto potenziale

L'impatto reale o potenziale esercitato sugli individui, sui gruppi o sull'insieme della società è una delle principali considerazioni da tenere presenti. Spesso, le ripercussioni negative subite dall'individuo o dal gruppo si rivelano più importanti della valutazione dell'episodio da parte di osservatori esterni.

Come intervenire?

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.

Occorre in tal senso fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, e promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network.

Si potrebbe, quindi, pensare ad attività di analisi e produzione mediale, finalizzate soprattutto a:

- 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.

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?

Secondo uno studio del King's College di Londra più del 23% dei giovani intervistati ha una relazione disfunzionale con il proprio smartphone. Stati d'ansia provocati dalla ricerca e dall'uso compulsivo del cellulare che, nei casi più gravi, si associano a veri e propri stati depressivi. In Italia, secondo una ricerca, ben il 45% degli studenti (6.671 giovani tra gli 11 e i 25 anni) dichiara di passare sul web almeno 5-6 ogni giorno e il tempo trascorso online raggiunge picchi più alti nel fine settimana: 1 intervistato su 5 dice di sentirsi a disagio o comunque va in ansia quando manca la connessione alla Rete e cresce in contemporanea la percentuale di coloro che manifestano attacchi di panico quando finiscono i giga e le promozioni tariffarie a cui sono abbonati (circa 1 su 3). Ancora, secondo l'Istat, *"nel 2018, l'85,8% dei ragazzi tra 11 e 17 anni di età utilizza quotidianamente il telefono cellulare. Il 72% dei ragazzi in quella stessa fascia di età naviga in Internet tutti i giorni. Questa quota è cresciuta molto rapidamente passando dal 56,2 al 72,0% nell'arco di un quadriennio. Le più frequenti utilizzatrici del cellulare e della rete sono le ragazze, l'87,5% delle quali usa il cellulare quotidianamente e il 73,2% accede a Internet tutti i giorni (quota che sale all'84,9% se ci si concentra sulle adolescenti tra i 14 e i 17 anni). L'accesso ad Internet è fortemente trainato dalla diffusione degli smartphone. Soltanto il 27,7% dei ragazzi, infatti, usa il pc tutti i giorni e questa quota è in forte calo rispetto al 40,5 del 2014"*.

La dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

La S.I.I.Pa.C., la Società Italiana Intervento Patologie Compulsive**, definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete; di seguito alcune caratteristiche specifiche:**

- **Dominanza**. L'attività domina i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi.
- **Alterazioni del tono dell'umore.** L'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza.

- **Conflitto**. Conflitti inter-personali tra il soggetto e coloro che gli sono vicini, conflitti intra-personali interni a se stesso, a causa del comportamento dipendente.
- **Ricaduta**. Tendenza a ricominciare l'attività dopo averla interrotta.

I segnali patologici di questo che viene descritto come **"un vero e proprio abuso della tecnologia"**, anche denominato **"Internet Addiction Disorder"** (I.A.D. coniato dallo psichiatra Ivan Goldberg 1996), sono specifici così come accade per le altre dipendenze più "tradizionali". In particolare, si hanno: la tolleranza ossia quando vi è un crescente bisogno di aumentare il tempo su internet e l'astinenza quando, cioè, vi è l'interruzione o la riduzione dell'uso della Rete che comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi (malessere psichico e/o fisico che si manifesta quando s'interrompe o si riduce il comportamento). Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

Da sottolineare, la nomofobia (nomo deriva da "no-mobile") termine usato per categorizzare quei soggetti che sperimentano emozioni negative, quali ansia, tristezza e rabbia quando non sono connessi con il proprio smartphone. Anche qui i dati dell'Osservatorio nazionale adolescenza sembrano parlare chiaramente: *"quasi 8 adolescenti su 10 hanno paura che si scarichi il cellulare o che non gli prenda quando sono fuori casa (un dato in forte crescita se si pensa che fino allo scorso anno interessava il 64% degli adolescenti) e tale condizione, nel 46% dei casi genera ansia, rabbia e fastidio. Questo fenomeno è meno diffuso tra i ragazzi più piccoli, tra gli 11 e i 14 anni, che si fermano ancora al 60% e solo il 32% sperimenta alti livelli di ansia e preoccupazione"*.

Spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale che può anche assumere forme di Dipendenza dal gioco online (Net gaming addiction o Internet Gaming Addiction) inserito all'interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM 5). Da specificare che la dipendenza qui si realizza quando c'è un abuso, ossia un utilizzo continuativo e sistematico della Rete al fine di giocare impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

In particolare, sei sono le componenti che a livello bio-psico-sociale possono portare ad una vera e propria dipendenza**. Di seguito i sintomi che devono essere presenti (per un arco di tempo di almeno un anno):**

- il giocatore è assorbito totalmente dal gioco;
- il giocatore è preoccupato e ossessionato dal gioco (si veda Lancini M., Il ritiro sociale negli adolescenti, Raffaello Cortina Ed., Milano, 2019);

- il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;
- il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;
- il giocatore sente di dover dedicare più tempo ai giochi;
- il giocatore se non può giocare manifesta ansia, depressione e irritabilità;
- può emergere un ritiro sociale (si veda il punto 3);
- il giocatore, anche se comprende la gravità della situazione e sospende di giocare comunque non riesce a interrompere del tutto;
- il giocatore mente agli altri sull'utilizzo che fa dei giochi on line;
- il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su Internet o ha perso interesse verso attività nella vita reale.

Anche in questo caso, 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.

La tecnologia infatti ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita. 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.

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.

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.

"Secondo una recente ricerca di Skuola.net, per la Polizia di Stato - ricerca che ha coinvolto 6.500 ragazzi tra i 13 e i 18 anni - il 24% di loro ha scambiato almeno una volta immagini intime con il partner via chat o social (fenomeno conosciuto come sexting). Tra questi, il 15% ha subito la condivisione con terzi, senza consenso, di questo materiale. Il motivo più frequente, riportato dalle vittime? Un banale "scherzo" (49%), a dimostrazione di quanto possano essere sottovalutate le reali conseguenze di tale diffusione. Tra le altre motivazioni, il ricatto (11%) o la vendetta (7%): il revenge porn, pure presente, viene surclassato dalla leggerezza e dalla goliardia ma gli effetti sono drammaticamente gli stessi. La reazione più diffusa nella maggior parte dei casi è il silenzio: il 53% ha fatto finta di niente, il 31% non ha detto nulla per non essere giudicato".

Il sexting (abbreviazione di sex – sesso e texting – messaggiare, inviare messaggi) indica l'invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri.

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 (la Legge 19 luglio 2019

n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Si veda l'articolo 612 ter del codice penale rubricato "Diffusione illecita di immagini, video sessualmente espliciti". Tra le caratteristiche del fenomeno vi sono principalmente:

- **la fiducia tradita:** chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);
- **la pervasività con cui si diffondono i contenuti:** in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;
- **la persistenza del fenomeno:** il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.

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.

L'importanza di un'adeguata educazione all'affettività e alla sessualità

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità.

Nella società digitale, attraverso la Rete, i minori definiscono se stessi, si raccontano e sperimentano nuove forme di identità, socializzano, si emozionano e si relazionano con gli altri, scoprono la propria sessualità e giocano con essa.

Tutto ciò risponde a bisogni assolutamente naturali e importanti, ma allo stesso tempo può esporre i ragazzi a possibili rischi come quello, appena approfondito, dell'adescamento online.

Il desiderio di conferma sociale (da ottenere anche attraverso i social) e, talvolta, la scarsa consapevolezza degli adolescenti nel gestire la propria immagine online quando pubblicano sui loro profili social video e foto piuttosto intimi o sensuali, può aumentare il rischio di esporli ad un adescamento online. Con un'adeguata competenza digitale ed emotiva, Internet potrebbe essere un valido supporto per

i/le ragazzi/e nel loro percorso di esplorazione della sessualità. Purtroppo, però, non è sempre così. La Rete, infatti, abbonda di contenuti inadeguati che offrono una rappresentazione distorta della sessualità e dei rapporti uomo-donna. La sessualità in Rete è spesso rappresentata in modo decontestualizzato e senza alcun richiamo alla dimensione affettiva ed emotiva dei soggetti. Il più delle volte, tali rappresentazioni ricalcano con forza stereotipi di genere come quello della "donna oggetto" e quello dell'"uomo forte e virile", tanto più forte e virile quanto più è in grado di conquistare e dominare quell'"oggetto".

In un contesto simile non c'è da stupirsi se, talvolta, anche i comportamenti degli adolescenti in Rete nella gestione della propria sessualità o semplicemente della propria immagine online riproducano tali modelli. Modelli che la società odierna sembra tuttora confermare in numerosi messaggi che quotidianamente ci arrivano attraverso i media.

La problematica dell'adescamento online (come quella del sexting), quindi, si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale, in riferimento al modo in cui i/le ragazzi/e vivono la propria sessualità e la propria immagine online, al loro desiderio di esprimersi e affermare se stessi.

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

Come intervenire?

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: 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.

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 coinvolte/i 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.

La pedopornografia esiste da prima dell'avvento di Internet. Tuttavia, la diffusione della Rete, l'evoluzione e la moltiplicazione dei "luoghi" virtuali, il cambiamento costante delle stesse tecnologie digitali, ha radicalmente cambiato il modo in cui il materiale pedopornografico viene prodotto e diffuso, contribuendo ad un aumento della sua disponibilità e dei canali di diffusione. La diffusione della banda larga,

ad esempio, consente di caricare e scaricare velocemente video e foto anche di grandi dimensioni, così come la diffusione delle videocamere e dei cellulari con videocamera incorporata, consente la produzione "in house" di materiale video, riproducibile facilmente online.

Sul versante nazionale, secondo dati ISTAT, nel 2015 sono state avviate 1.032 indagini per il reato di atti sessuali con minorenni, nonché 720 per pornografia minorile.

Secondo i dati della Polizia Postale del 2017, nell'ambito della pedopornografia online, sono state registrate 532 denunce e 43 arresti. Dalle complesse operazioni di prevenzione della Polizia di Stato, è scaturita una assidua attività di monitoraggio della Rete, che ha visto coinvolti ben 28.560 siti internet, di cui 2.077 inseriti nelle black list. Si conferma la rilevanza del fenomeno dell'adescamento di minori online che ha registrato 437 casi trattati che hanno portato alla denuncia di 158 soggetti e all'arresto di 19. Nel corso dell'anno 2018 i siti Internet segnalati sono aumentati sino ad arrivare a 33.086, di cui 2.182 inseriti nelle black list.

Qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione "Segnala contenuti illegali". 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, se si ravvisa un rischio per il benessere psicofisico dei/lle bambini/e, ragazzi/e coinvolte 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 Stao - 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. Si pensi, a titolo di esempio, all'impatto che può avere la consapevolezza dell'esistenza (spesso anche in Rete) delle immagini e/o video dell'abuso sulla vittima, o a come gestire le stesse immagini e/o video durante la fase investigativa e giudiziaria. L'esposizione alle immagini dell'abuso, infatti, sia durante il processo giudiziario, sia durante il percorso di cura, deve essere attentamente valutata, poiché può comportare, per il/la minore coinvolto/a, un rischio di vittimizzazione secondaria.

Negli ultimi anni, infine, abbiamo assistito all'emergere di un altro fenomeno che può avere risvolti connessi al fenomeno della pedopornografia: il sexting, di cui abbiamo parlato nelle precedenti lezioni. La mancanza di intenzione di danneggiare o sfruttare l'altro/a (anche se a volte tale materiale può essere successivamente utilizzato con questo scopo come nel caso del cyberbullismo o del ricatto a fini di estorsione) non esclude che i comportamenti del sexting possano configurare reati connessi con la pedopornografia poiché, secondo il nostro ordinamento giudiziario, il materiale così prodotto e scambiato si declina come pedopornografico e soprattutto perché il rischio di perdere il controllo di tali immagini, uscendo dallo scambio consensuale è molto alto e spesso ragazzi e ragazze non hanno consapevolezza delle conseguenze (anche serie) delle loro azioni, come la possibilità di diffondere in Rete immagini intime/private di altri/e fuori dai canali riservati dello scambio.

Secondo il recente parere emesso del Comitato di Lanzarote del Consiglio d'Europa (l'organismo incaricato di monitorare l'attuazione della Convenzione del Consiglio d'Europa sulla protezione dei/lle bambini/e contro lo sfruttamento e gli abusi sessuali), il "sexting" tra minori (generare, ricevere e condividere in modo consensuale immagini/video a sfondo sessuale o sessualmente espliciti di sé stessi attraverso le tecnologie digitali) non costituisce una condotta connessa alla "pedopornografia", se destinato esclusivamente all'uso privato dei minori, tuttavia se il materiale privato dovesse essere diffuso si configurerebbe invece come pedopornografico. Il parere specifica inoltre che i minori costretti a tale condotta dovrebbero essere affidati ai servizi di assistenza alle vittime e non essere perseguiti penalmente e che particolare attenzione andrebbe posta, nel caso tale

materiale fosse prodotto tra bambini/e.

Al di là delle interpretazioni della giurisprudenza in merito, il fenomeno dei sexting di cui abbiamo parlato nelle precedenti lezioni richiede più utilmente di porre l'attenzione sulla necessità della prevenzione: i più giovani devono acquisire quelle competenze in grado di orientarli e guidarli nelle loro scelte anche online**; per questo motivo, come già sottolineato, l'educazione, compresa l'educazione all'affettività, riveste un ruolo fondamentale.**

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. Ad esempio, non è utile diffondere tra i bambini e le bambine più piccoli/e l'uso di servizi come le hotline, sia perché in caso di visione accidentale di materiale pedopornografico è opportuno che bambini/e e ragazzi/e possano parlarne con gli adulti di riferimento per la migliore risposta possibile, sia perché si potrebbe incentivare la ricerca proattiva, che comunque è vietata dalla legge italiana, per minori e per adulti.

Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio.

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 delle hotline.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

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

☐ 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.

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.

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

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

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/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 alunni possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni o di altri e riferire spontaneamente o su richiesta l'accaduto ai docenti. I fatti riferiti possono essere accaduti anche al di fuori della scuola. Anche confrontandosi periodicamente con gli alunni sui rischi delle comunicazioni online, i minori possono riferire di fatti o eventi

personali o altrui che “allertano” l’insegnante. Una “prova” di quanto riferito può essere presente nella memoria degli strumenti tecnologici utilizzati, può essere mostrata spontaneamente dall’alunno, può essere presentata da un reclamo dei genitori, può essere notata dall’insegnante che si accorge dell’infrazione in corso. Il docente è autorizzato a controllare le strumentazioni della scuola, mentre per controllare l’uso del telefono cellulare di un bambino, egli si rivolge al genitore.

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 (l’eventuale tefefonino/smartphone personale e il pc collegato a internet) per i bambini possono essere i seguenti:

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

5.2. - Come segnalare: quali strumenti e a chi

L’insegnante riveste la qualifica di pubblico ufficiale in quanto l’esercizio delle sue funzioni non è circoscritto all’ambito dell’apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all’uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.

Gli insegnanti, anche con l'ausilio tecnico dell'Animatore digitale, possono provvedere ugualmente a conservare le prove della condotta incauta, scorretta o dell'abuso rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto.

Qualora ci si dovesse accorgere che l'alunno, usando il computer, 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 documento word.

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 alunni, al Dirigente scolastico e, per le condotte criminose, alla polizia.

Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e per fatti rilevanti anche al Dirigente scolastico; per quelle criminose, anche alla polizia.

In particolare la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.

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

1. Annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata.

2. Convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti.

3. Relazione scritta al Dirigente scolastico.

In base all'urgenza, le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi. Inoltre, per i reati meno gravi, la legge rimette ai genitori degli alunni la scelta di richiedere la punizione del colpevole attraverso la querela.

Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia 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.

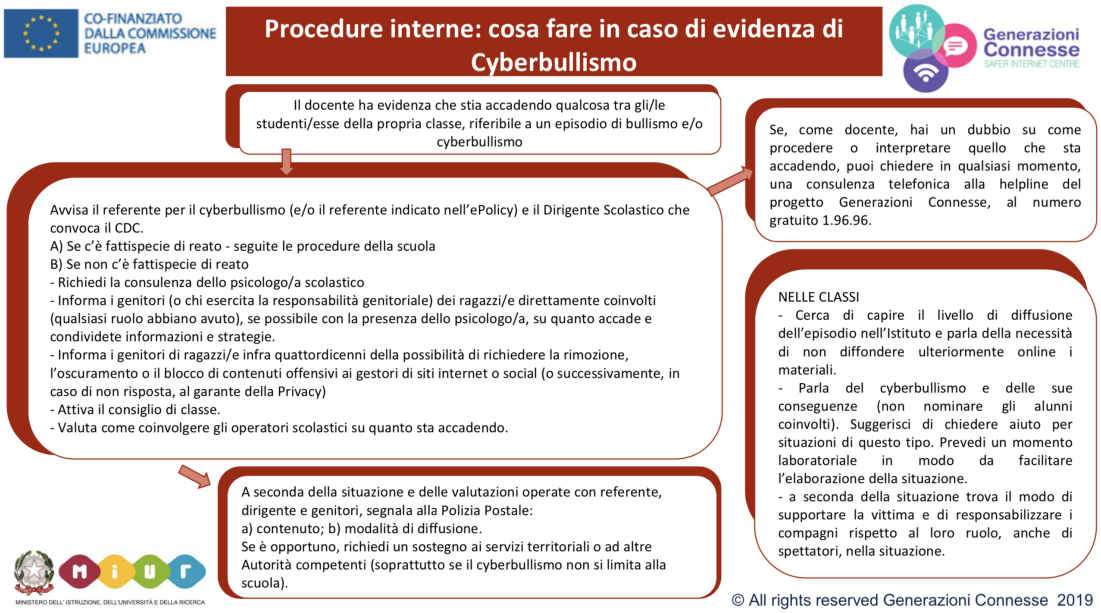
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

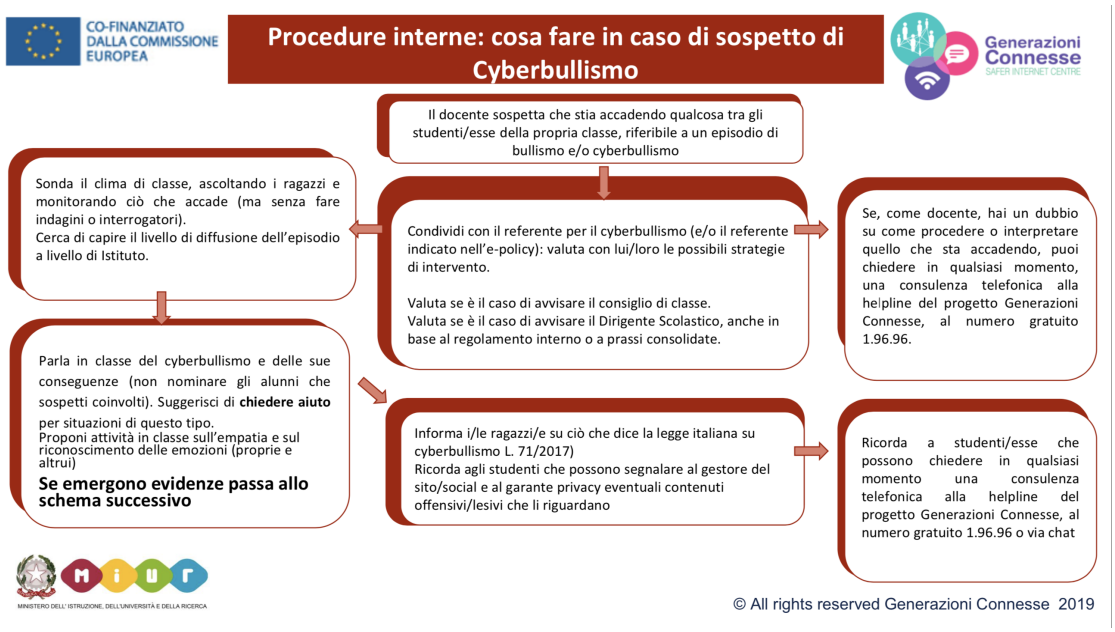
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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.

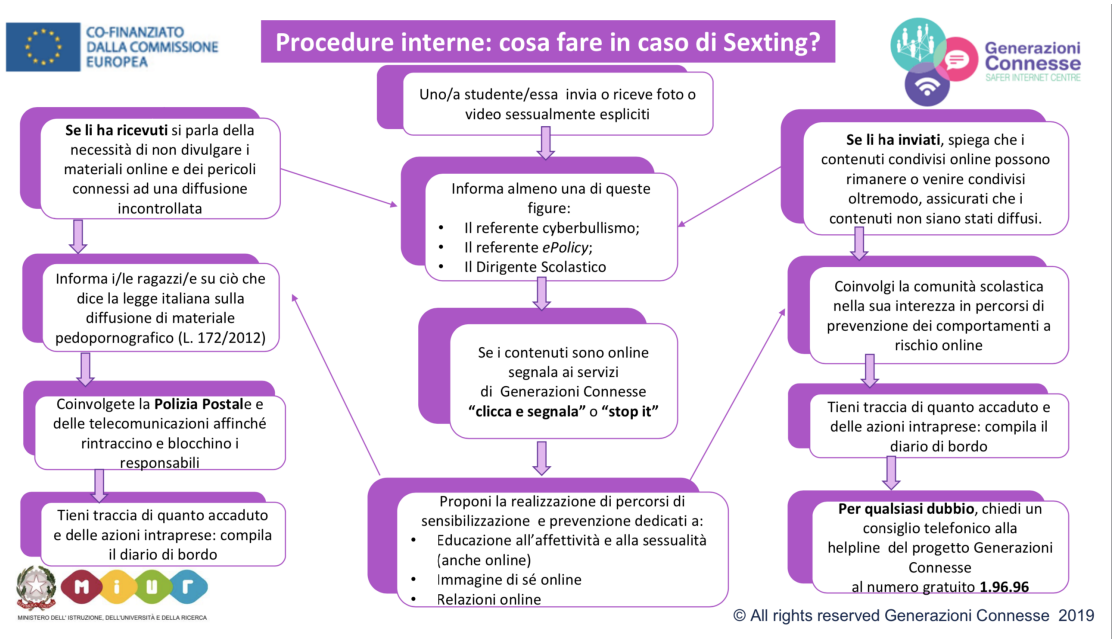
5.4. - Allegati con le procedure

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

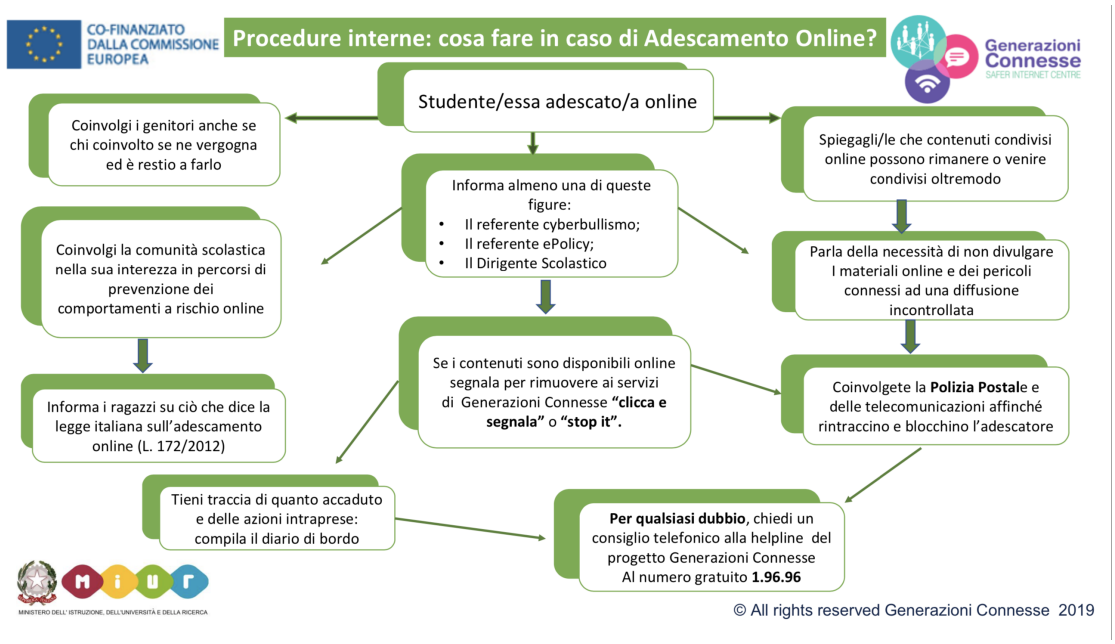




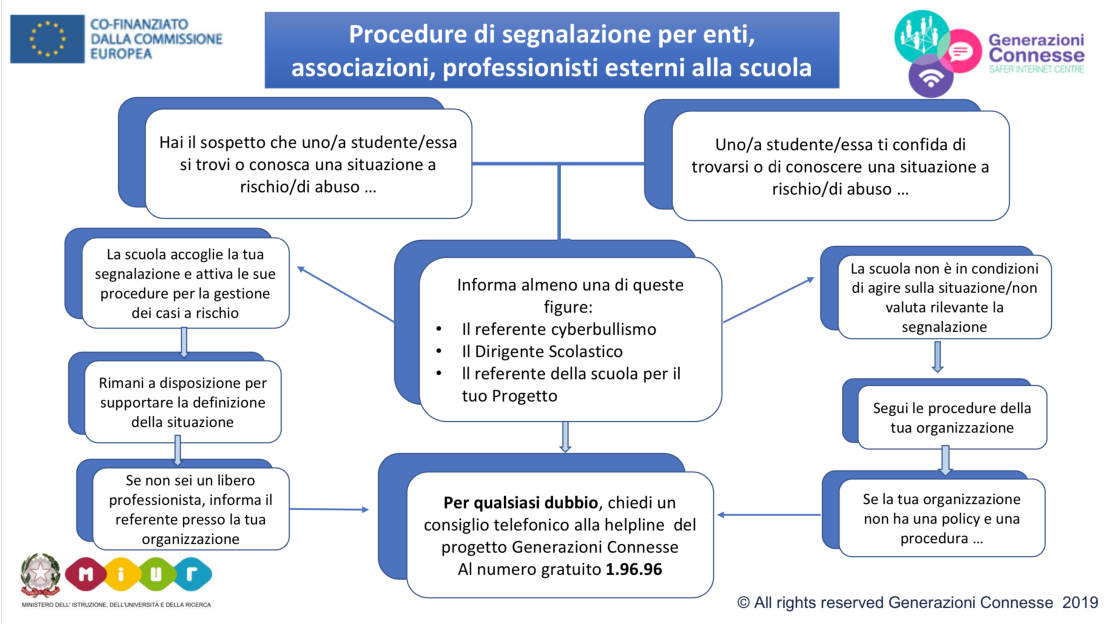
Procedure interne: cosa fare in caso di sexting?



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

L'Istitutosi impegna ad informare gli stakeholder attraverso:

- interventi di esperti
- incontri di formazione ed informazione