Istituto Comprensivo
Santa Chiara
Pascoli - Altamura
Foggia

Documento di ePolicy

FGIC877005

S. CHIARA - PASCOLI - ALTAMURA

PIAZZA S.CHIARA N.9 - 71121 - FOGGIA - FOGGIA (FG)

Mariolina Goduto

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.

Scopo del presente documento di ePolicy è di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della

normativa vigente. Educare alla cittadinanza digitale è un dovere per la scuola condiviso con la famiglia e allargato a tutta la Comunità Educante. 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 procedure e competenze "tecniche", ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali, al fine di formare i futuri cittadini della società in un mondo sempre più connesso.

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

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

Per la sua natura, legata ad una realtà in continua evoluzione come quella delle risorse digitali e delle opportunità didattiche da esse offerte, la presente Policy è aperta ad implementazioni e revisioni di carattere annuale, accogliendo segnalazioni e suggerimenti.

1.2 - Ruoli e responsabilità

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

Il Dirigente Scolastico si impegna per garantire la sicurezza, anche online, di tutti i membri della comunità scolastica. È formato adeguatamente sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR; promuove la cultura della sicurezza online e, insieme all'Animatore Digitale e al docente referente sulle tematiche del bullismo/cyberbullismo, propone corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Inoltre, 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 supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento anche 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 ha il compito di controllare che gli utenti autorizzati usino gli account forniti dall'Istituto e accedano alla Rete della scuola con apposita password solo per scopi istituzionali e consentiti (istruzione e formazione).

Il Referente bullismo e cyberbullismo ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi 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 (ove possibile) può coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori. Monitorerà i materiali utilizzati per facilitare tra gli studenti l'espressione di eventuali disagi come, a titolo esemplificativo, lettere depositate nelle Bully-Boxes, appunti di colloqui svolti in cerchio, questionari di rilevazione. Curerà l'aggiornamento periodico dello schema riepilogativo delle situazioni gestite legate a rischi online.

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Sono tenuti a integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica soprattutto alla luce del documento della "Didattica digitale integrata". I docenti hanno il dovere di accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della Classroom e della app di Google nonché dei Chromebook quali dispositivi tecnologici che si connettono alla GSuite attivata dalla scuola, in particolare hanno i dovere di garantire agli studenti una didattica digitale integrata secondo quanto disposto nel documento ddi approvato in Collegio; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

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 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. È coinvolto nelle attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA può essere coinvolto, infine, 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, in relazione al proprio grado di maturità e consapevolezza raggiunta, si impegnano a utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola, devono approfondire come tutelarsi online, tutelare i/le compagni/e e rispettarli/le; partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e a farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education; evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali; segnalare ogni abuso, uso improprio o accesso a materiali inappropriati tenendosi informati sul protocollo per tali segnalazioni.

I Genitori, in continuità con l'Istituto scolastico, devono essere partecipi e attivi nelle attività di

promozione ed educazione sull'uso consapevole delle TIC e della GSuite (account, Classroom e Google apps), nonché sull'uso responsabile dei device personali ricevuti in comodato d'uso dalla scuola; devono relazionarsi 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. Sottoscrivendo il patto di corresponsabilità, si impegnano ad accettare e condividere quanto scritto nell'ePolicy dell'Istituto.

Gli Enti educativi esterni e le Associazioni verranno resi edotti circa la politica d'Istituto riguardo all'uso consapevole della Rete e delle TIC, confidando nella loro collaborazione per la divulgazione di comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme. Tutti gli attori che entreranno in relazione educativa con gli studenti dovranno mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati; di essere guidati dal principio di interesse superiore del minore; di ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa. In particolare dovranno adeguarsi alle indicazioni ad hoc e procedure standard elencate nella ePolicy per il coinvolgimento di attori esterni nel paragrafo successivo (1.3)

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 linea con i principi di corresponsabilità educativa l'Istituto si impegna a produrre un'informativa sintetica sull'ePolicy, comprensiva delle procedure di segnalazione da condividere con tutte le figure

che operano con gli studenti, non solo per tutelare questi ultimi e la scuola stessa, ma anche per porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali. Tale documento chiarirà il sistema di azioni e le procedure di segnalazione da seguire da parte di professionisti ed organizzazioni esterne, consentendo di distinguere i ruoli e le azioni da compiere e da attivare. Le procedure di segnalazione dovranno contenere i riferimenti interni alla scuola a cui rivolgersi in tali situazioni (il dirigente, il referente cyberbullismo, il referente del progetto, il coordinatore di classe). L'informativa espliciterà le modalità di utilizzo dei dispositivi personali (smartphone, tablet, pc, etc.) e di quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti. Il documento metterà in evidenza l'obbligo di rispettare la privacy. Le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività devono prendere visione di tutti i documenti proposti dall'Istituto e sottoscriverli preliminarmente all'avvio dei programmi con gli studenti e le studentesse, in classe o fuori.

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.

L'Istituto potrà attuare anche altre modalità di condivisione e comunicazione come:

- l'affissione di manifesti disponibili sul sito Generazioni Connesse;

- la distribuzione di opuscoli agli studenti e ai genitori, disponibili sul sito Generazioni Connesse;

- un incontro collegiale dei docenti per illustrare contenuti e pratiche; una verifica annuale per apportare modifiche, integrazioni ed elaborare eventuali protocolli di intervento;

- un incontro annuale con i genitori per sensibilizzare sui temi della sicurezza informatica e illustrare i comportamenti da monitorare o evitare; durante l'incontro può essere consegnato il Patto di Corresponsabilità

- una discussione in classe nei primi giorni di scuola, con gli studenti, sul documento di ePolicy; inserimento di un estratto del documento nel diario scolastico, con particolare riguardo ai comportamenti da tenere in caso di bisogno.

Per condividere in modo efficace il documento con tutta la comunità educante, ponendo al centro gli studenti e sottolineando compiti, funzioni e attività reciproche verrà redatta una versione Child Friendly del documento, con un linguaggio e modalità comunicative adeguate a bambini e ragazzi. Il documento verrà illustrato e consegnato durante gli incontri scuola-famiglia e condiviso con gli studenti in classe.

1.5 - Gestione delle infrazioni alla ePolicy

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

Le infrazioni alla ePolicy potranno essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure potranno essere segnalate da alunni e genitori a docenti/ATA, dandone tempestiva segnalazione al Dirigente Scolastico. Nel caso in cui le infrazioni della ePolicy violino norme previste dal Regolamento di Istituto si procederà secondo quanto previsto dal regolamento stesso. Qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola interverrà secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di accoglienza, recupero ed educazione. Riteniamo di fondamentale importanza, in situazioni di infrazioni alla ePolicy, intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione, per promuovere una maggiore consapevolezza e mantenere un clima di classe attivo, partecipativo, solidale, responsabile e aperto alla gestione dei conflitti nel rispetto delle persone e delle relazioni. In accordo con i genitori verrà inoltre assicurato un immediato supporto psicologico allo studente attraverso i servizi predisposti, qualora ciò fosse ritenuto necessario.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

La policy richiede l'integrazione con l'inserimento delle seguenti norme: utilizzo del laboratorio di informatica, delle postazioni di lavoro e dell'utilizzo di internet-

Disposizioni sull'uso del laboratorio

1. Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.

2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.

3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando l'orario di ingresso, quello di uscita e motivazione dell'uso delle postazioni informatiche. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.

4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.

5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.

6. Nei laboratori è vietato utilizzare CD personali o dischetti se non dopo opportuno controllo con sistema di antivirus aggiornato.

7. È vietato cancellare o alterare files-dati presenti sull'hard disk.

8. Il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il mobilio in ordine, le

macchine spente correttamente (chiudi sessione…).

9. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.

10. In caso di malfunzionamento non risolvibile dal responsabile di laboratorio si contatterà personalmente o attraverso il Responsabile di laboratorio, la segreteria.

11. Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso. Si consiglia pertanto di salvare i dati importanti su Cd o pen drive periodicamente. In caso di formattazione ordinaria ci sarà un preavviso.

Disposizioni sull'uso dei software

1 I software installati sono ad esclusivo uso didattico.

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

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

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

Accesso a internet

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

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

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

4 È vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.

Norme finali

Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

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.

Saranno previsti due incontri annuali del Gruppo ePolicy per analizzare lo stato di attuazione dei seguenti punti e attivare le modifiche e gli interventi necessari:

promozione delle competenze digitali e dell'uso delle TIC nei percorsi educativi e didattici scolastici ed extrascolastici; prevenzione e gestione dei rischi online; percorsi di corresponsabilità educativa;

attività informative per promuovere la crescita di una cultura digitale consapevole; attività di formazione specifica per genitori e utenti esterni;

connessione e coerenza tra i vari documenti istituzionali, da allegare alla ePolicy;

coerenza ed efficacia comunicativa dei documenti rivolti a studenti, genitori, utenti esterni.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Azioni da svolgere nei prossimi 3 anni:

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

Capitolo 2 - Formazione e 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.

La progettazione di un curricolo sulle competenze digitali è scaturita dalla piena consapevolezza di cosa s'intende per "competenze digitali". 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, nel Curricolo si fa riferimento ad un framework comune per le competenze digitali e l'educazione ai media degli studenti e delle studentesse. I documenti di 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:

1. Aree di competenze individuate come facenti parte delle competenze digitali;
2. Descrittori delle competenze e titoli pertinenti a ciascuna area (21 competenze);
3. Livelli di padronanza per ciascuna competenza (i livelli sono 8);
4. Conoscenze, abilità e attitudini applicabili a ciascuna competenza;
5. 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.

Dall'analisi di questi documenti è scaturita la progettazione di un curricolo digitale della scuola che sarà oggetto di implementazione ogni qualvolta se ne rileverà la necessità.

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". Quale livello di competenza vogliamo che i nostri studenti raggiungano? Qual è il livello di competenza che i docenti devono acquisire per accompagnare studenti e studentesse in questo percorso? 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 favorire la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (ad es. con l'aiuto dell'animatore digitale e del Team dell'Innovazione) dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dai docenti (anche online), purché restino coerenti con il piano di formazione.

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 in modo da rispondere ai diversi bisogni formativi della classe.anche grazie alla possibilità di formazione permanente offerta loro in primis dall'Istituto scolastico, che prevede nel Piano di Formazione dei Docenti diverse opportunità di sviluppo professionale e aggiornamento tra cui:

- il percorso rinnovato con ciclicità annuale "Caffé digitale" a cura dell'Animatore Digitale.

- la formazione sulla Classroom di GSuite e delle relative applicazioni a cura dell'AD e del TI
- I percorsi formativi su metodologie didattiche innovative di Avanguardie Educative a cura dell'AD e del TI
- le opportunità di aggiornamento annulare in occasione del Safer Internet Day
- i percorsi laboratoriali di eTwinning e Erasmus plus

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.

Tale formazione 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 mettano al centro i temi in oggetto, considerando:

- percorsi di autoaggiornamento personali o collettivi,
- iniziative seminariali con professionisti-esperti interni (si pensi al supporto dell'Animatore digitale durante la settimana del Safe Internet Day) 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.

Tali azioni programmatiche sono inserite nel Piano triennale dell'offerta formativa.

L'Istituto ha in programma anche omenti 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 potrebbero essere 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 prevede la realizzazione di un cronoprogramma che consideri il triennio scolastico, in un'ottica di vera e propria programmazione, con azioni specifiche. Per esempio:

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

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

Sempre sul sito istituzionale della scuola, è incluso il link e materiali informativi del progetto "**Generazioni connesse**": 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.

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.

Oggi più che mai è importante rinforzare l'alleanza educativa fra scuola e famiglie.

Nella stesura di questo paragrafo dell'ePolicy abbiamo riflettuto sull'importanza del coinvolgimento delle famiglie nell'educazione digitale degli studenti e delle studentesse, con percorsi da mettere in pratica insieme per sensibilizzare i genitori sulle tematiche relative alle TIC.

Un primo passo in tal senso è quello di aggiornare o integrare, oltre che il regolamento scolastico, anche il "Patto di corresponsabilità", con specifici riferimenti alle tecnologie digitali e all'ePolicy.

Il "Patto di Corresponsabilità" è un documento centrale per ogni istituzione scolastica e per la comunità educante tutta. Per questo, recentemente è stato avviato dal Miur un percorso di revisione finalizzato a definire in modo più dettagliato modalità, tempi e ambiti della partecipazione da parte di genitori e studenti alla vita scolastica. E ciò, anche al fine di creare una maggiore collaborazione e condivisione degli interventi di formazione e di contrasto al bullismo e al cyberbullismo all'interno della comunità educante.

Per chiarire meglio il percorso di revisione del "Patto di Corresponsabilità" il MIUR ha pubblicato le Linee di indirizzo "Partecipazione dei genitori e corresponsabilità educativa". Il "Patto di Corresponsabilità educativa", si legge, punta a "rafforzare il rapporto scuola/famiglia in quanto nasce da una comune assunzione di responsabilità e impegna entrambe le componenti a condividerne i contenuti e a rispettarne gli impegni".

Aggiornare il "Patto di corresponsabilità" con specifici riferimenti all'uso delle tecnologie digitali e all'ePolicy è fondamentale, quindi, per informare e rendere partecipi le famiglie sul percorso che volete intraprendere con il documento e il piano d'azione.

A tale proposito è importante informare i genitori sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli.

Ad esempio, il Team dell'Innovazione ha in programma di:

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

- **prevedere azioni e strategie per il coinvolgimento delle famiglie** in tali percorsi di sensibilizzazione, ad esempio, mediante l'organizzazione di iniziative in cui anche gli studenti e le studentesse siano protagonisti.

Una particolare attenzione potrà essere dedicata a consigli, indicazioni e informazioni su iniziative e azioni della scuola, in riferimento ai rischi connessi ad un uso distorto della Rete da parte degli studenti e delle studentesse.

Ciò in continuità anche con l'art. 5 (comma 2) della legge 29 maggio 2017, n.71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che prevede l'integrazione, oltre che del regolamento scolastico, anche del "Patto di Corresponsabilità", con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari "commisurate alla gravità degli atti compiuti", al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

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

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

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.

Appare utile qui chiarire 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.

L'istituzione scolastica può 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).

La scuola ha 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 la scuola verifichino i loro trattamenti, controllando se i dati siano eccedenti rispetto alle finalità perseguite.

A tal fine il nostro Istituto Scolastico, al fine di allinearsi al Regolamento UE 2016/679 in merito all'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti, ha come obiettivi:

- Elaborazione e gestione di 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 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.
- Cura del processo sulla raccolta/gestione del consenso tramite un adeguamento di tutta la modulistica al Regolamento UE 2016/679 e la predisposizione di una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.

Attraverso il rifacimento del sito web istituzionale, inoltre, il nostro Istituto ha come obiettivo azioni di l'allineamento alla normativa vigente, 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);

Sulla messa in sicurezza della intranet scolastica si propongono interventi su

a) 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 (componente hardware che, utilizzando un certo insieme di regole predefinite, permette di filtrare ed eventualmente bloccare tutto il traffico da e verso una qualsiasi rete di computer, lasciando passare solo tutto ciò che rispetta determinate regole);

f) istituzione di 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 si terrà contoo nel momento della consultazione.

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.

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

Il primo passo è stato 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.

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 si ritiene 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 (nei tre plessi), 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.

Obiettivo del Gruppo di lavoro nel lungo termine, in ordine ad un aggiornamento dell'infrastruttura di rete, è 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, di cui il Gruppo di lavoro si farà carico, 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).

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.

A tal fine il Gruppo di lavoro si impegna ad inserire tra gli allegati dell'ePolicy un regolamento d'Istituto sull'uso delle TIC e sull'uso dei Laboratori di Informatica e Ambienti Innovativi.

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 la scuola provvede a pianificare interventi periodici di manutenzione e tiene anche un registro delle problematiche incontrate per poter stilare una classifica dei problemi più frequenti. Questo aspetto è fondamentale per permettere all'Animatore Digitale e ai membri del Team dell'Innovazione 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. Si ritiene opportuno a tal fine coinvolgere il tecnico della scuola (con contratto privato o occasionalmente da reti di scuole), in collaborazione con l'animatore digitale e il Team dell'Innovazione.

La formazione dovrebbe anche aiutare a familiarizzare con i dispositivi, laddove ci fossero incertezze e difficoltà. Si auspica pertanto che i docenti dell'Istituto partecipino più attivamente alle proposte

formative inserite del Piano di Formazione della scuola.

Ad esempio, si pensi, alla frequentazione di ambienti atelier digitali e creativi, alle "aule digitali" realizzate 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, oltre allo smartphone. Possono essere utilizzati in gruppo tablet o computer, 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 vengono elencate in modo puntuale le regole 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 prevede 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.

Il regolamento, dunque, prevede 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.

Inoltre il nostro Istituto, avendo attivato la GSuite for Educational, ha elaborato (su iniziativa dell'AD) un apposito Regolamento sull'uso della GSuite per docenti e studenti nonché un documento sulla privacy per l'attivazione delgli account con estensione @scuolasantachiara.edu.it per tutti gli utenti: Studenti, Docenti, alcune figure di genitori e il personale ATA.

Ricordiamo che la legge Ferrara, la legge 71 del 29 maggio 2017, chiede alle scuole di aggiornare il patto di corresponsabilità, per cui è stato inserito un punto specifico relativo all'uso della connessione Internet della scuola. La scuola informa 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.

La scuola non può non sviluppare un proprio regolamento o decidere di non usare la tecnologia a scuola: il curricolo scolastico prevede che gli/le studenti/esse imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le ICT. Ma ciò non è sufficiente: 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, la nostra scuola offre sia agli/lle studenti/esse che agli insegnanti opportunità di scambi culturali con gli/le studenti/esse di altri Paesi e l'Animatore Digitale, anche in qualità di Ambasciatore eTwinning si occupa di 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.

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 il Gruppo di lavoro si occuperà 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. L'obiettivo è 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.

Si troverà il modo affinché queste informazioni sulla sicurezza in Internet a scuola vengano 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.

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, la pagina Facebook, la App "Santachiaramagazine!. Tali strumenti, naturalmente, possono essere utilizzati anche per fornire informazioni di servizio rivolte a studenti o genitori. Il Gruppo di lavoro prevede un coordinamento affinché la comunicazione esterna online della scuola sia condivisa e 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, se 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 dovrà essere prevista dalla contrattazione di Istituto.

A titolo esemplificativo, sullo stesso tema si allega a questo documento ePolicy un interessante "Manifesto per un uso consapevole di 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).***

Il Gruppo di lavoro sta elaborando un documento da allegare al documento ePolicy sulle modalità e alcune indicazioni utili su come dovrebbe essere utilizzato il registro elettronico nel nostro Istituto. Sarebbe molto importante, infatti, che tale strumento venisse usato sfruttandone appieno le potenzialità, al fine di rendere quanto più immediate, trasparenti ed efficaci le comunicazioni all'interno della scuola e fra scuola e famiglie.

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". (Ansa, "Cellulare in aula, 1 su 2 lo usa con prof.", del 26.01.2018).

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…), violandone la privacy.

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.

"La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficace".

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.

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

1. **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
2. **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.
3. **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.
4. **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.
5. **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.
6. **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.
7. **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.

8. **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.
9. **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.
10. **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, 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, il Gruppo si lavoro si occuperà di 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 deglistudenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte delpersonale Tecnico Amministrativo e dagli ATA

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

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

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 consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto

dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Il bullismo e il cyberbullismo sono fenomeni dalla portata ampia e complessa, che chiamano in causa dinamiche complesse, riconducibili essenzialmente alla capacità di gestione del confronto e della relazione con il Sé e l'altro e possono coinvolgere anche la dimensione affettivo-relazionale e quella sessuale. La comunità educante, in questo ambito può e deve cercare di lavorare in maniera reticolare, coinvolgendo nel processo di sensibilizzazione tutti gli attori e le agenzie territoriali: famiglia, studenti e studentesse, Forze dell'Ordine, ASP del terzo settore rappresentano i "nodi" strategici per la diffusione di pratiche sostenibili legate all'utilizzo consapevole e critico delle TIC.

Coscienza dei rischi e conoscenza delle potenzialità sono i due poli della sfida educativa e del

cammino di crescita da percorrere in un'ottica di condivisione e di corresponsabilità con la famiglia e con il territorio per socializzare un capitale umano ad alto tasso di democrazia e civismo.

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).

Gli atti di cyberbullismo possono essere suddivisi in due fattispecie diverse:

1. c. diretto: il bullo utilizza strumenti di messaggistica istantanea come SMS o MMS, che hanno un effetto immediato sulla vittima poiché diretti esclusivamente alla persona;
2. c. indiretto: il bullo fa uso di spazi pubblici della Rete, come Social network, blog o forum,

per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima, anche dal punto di vista psicologico.

È utile riportare alcuni tra i segnali che la vittima potenziale di cyberbullismo può manifestare:

- appare nervoso/a quando riceve un messaggio o una notifica;
- sembra a disagio nell'andare a scuola o finge di essere ammalato/a (ha spesso mal di stomaco o mal di testa);
- cambia comportamento ed atteggiamento in modo repentino;
- mostra ritrosia nel fornire informazioni su ciò che fa online;
- mostra rabbia o appare depresso/a dopo essere stato/a online;
- utilizza sempre meno PC e telefono (arrivando ad evitarli);
- perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- peggioramento del suo rendimento scolastico.

Chi commette atti di bullismo è penalmente perseguibile per i seguenti reati, così come riportato nel Codice penale:

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

Scuola e famiglia devono esercitare un'attenzione costante e mettere a punto sistemi di valutazione dei segnali di malessere, in modo da prevenire, arginare ed evitare l'insorgere di possibili dinamiche critiche. Accanto al sistema di segnalazione e di accompagnamento appare fondamentale condurre un'azione periodica di sensibilizzazione aprendo la comunità educante all'incontro con Enti, APS e soggetti istituzionali che operano nel settore della prevenzione e del contrasto al bullismo e al cyberbullismo.

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.

Il contrasto alle tipologie di hate speech passa attraverso una strategia basata sul decentramento cognitivo, sull’abbattimento degli stereotipi, sulla conoscenza fenomenologica e sul protagonismo sociale, inteso come possibilità di apprendere e praticare la comunicazione non ostile, declinandola in ambito scolastico e familiare. Conoscere, conoscersi e comunicare sono tre ambiti intimamente legati tra di loro e permettono di praticare quella decostruzione dal basso degli stereotipi legati alla razza, al genere, all’orientamento sessuale, alla disabilità. Le forme di hate speech si manifestano sempre più spesso e sono veicolate attraverso il mondo dei media digitali e dei social network. L’Istituto dovrà allora promuovere una partecipazione civica e attiva strutturando percorsi di attività mirate a svelare le forme di hate speech e un esercizio costante, da praticare anche attraverso l'impegno delle famiglie, per la promozione e il ricorso ad una comunicazione diversa, attiva e positiva.

4.4 - Dipendenza da Internet e gioco online

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

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

La formazione del personale rappresenta una delle leve strategiche attraverso le quali l’Istituto realizza gli obiettivi processo fissati nei documenti programmatici e persegue la strategia complessiva di filosofia pedagogica, attenta anche al benessere digitale sia degli studenti che delle famiglie. Nel corso del prossimo triennio saranno monitorati gli indicatori specifici relativi alla

dipendenza da Internet e verranno implementate delle proposte di formazione per riconoscere ed intervenire in maniera tempestiva sulle dinamiche non fisiologiche legate a questa forma di dipendenza, cercando di coinvolgere le famiglie, che in merito a questo aspetto costituiscono un osservatorio privilegiato delle abitudini degli studenti e delle studentesse.

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.

Da implementare con le indicazioni contenute nella lezione.

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.

Breve vademecum per riconoscere un eventuale caso di adescamento online.

È importante prestare attenzione a piccoli segnali che possono essere indicatori importanti nella valutazione di un cambiamento improvviso nel comportamento di un minore:

1. Il minore ha conoscenze sessuali non adeguate alla sua età?
2. Si viene a conoscenza di un certo video o di una foto che circola online o -ancora- il minore ha ricevuto un contenuto (o filmato), ma c'è imbarazzo e preoccupazione nel raccontare di più all'adulto?
3. Il minore si isola totalmente e sembra preso solo da una relazione online?
4. Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?

Se si ritiene che sussistano le condizioni per un eventuale adescamento si attivano tutte le procedure preposte (riportate nel presente documento) e si coinvolgono tutti gli attori interessati per approfondire la situazione.

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.

Da implementare con le indicazioni contenute nella lezione.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

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

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

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

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

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

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

☐ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della

diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

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

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

Scegliere almeno 1 di queste azioni:

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

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

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

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

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

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

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

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

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.

I contenuti "pericolosi" per gli alunni possono essere i seguenti:

- contenuti che violino la 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 che implichino la sfera della sessualità

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

- annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata;
- convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;
- relazione scritta al Dirigente scolastico.

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.

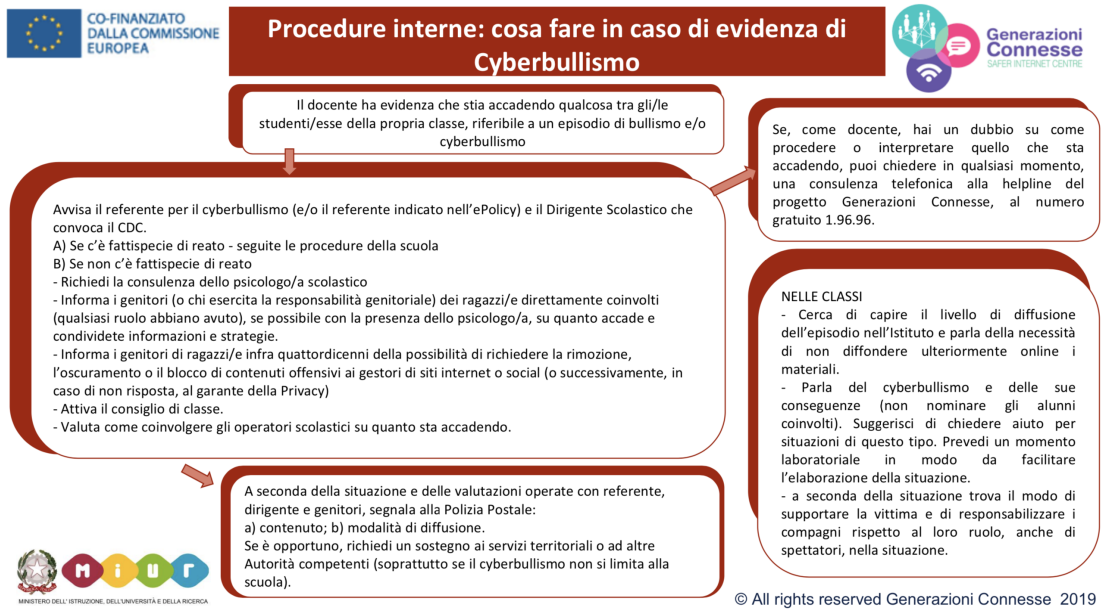
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza 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.

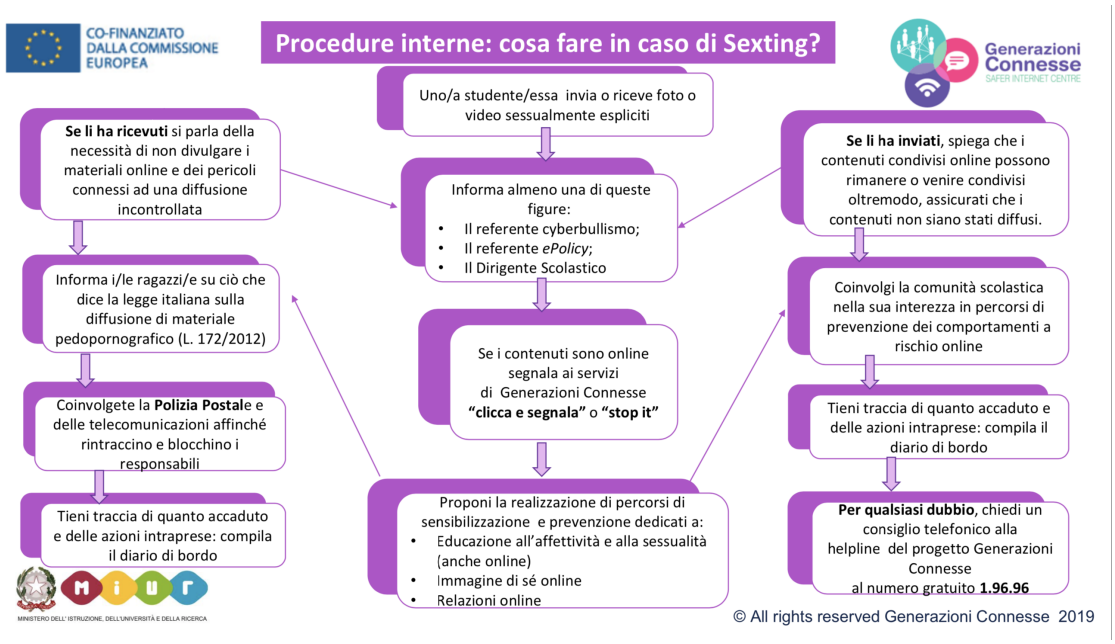
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

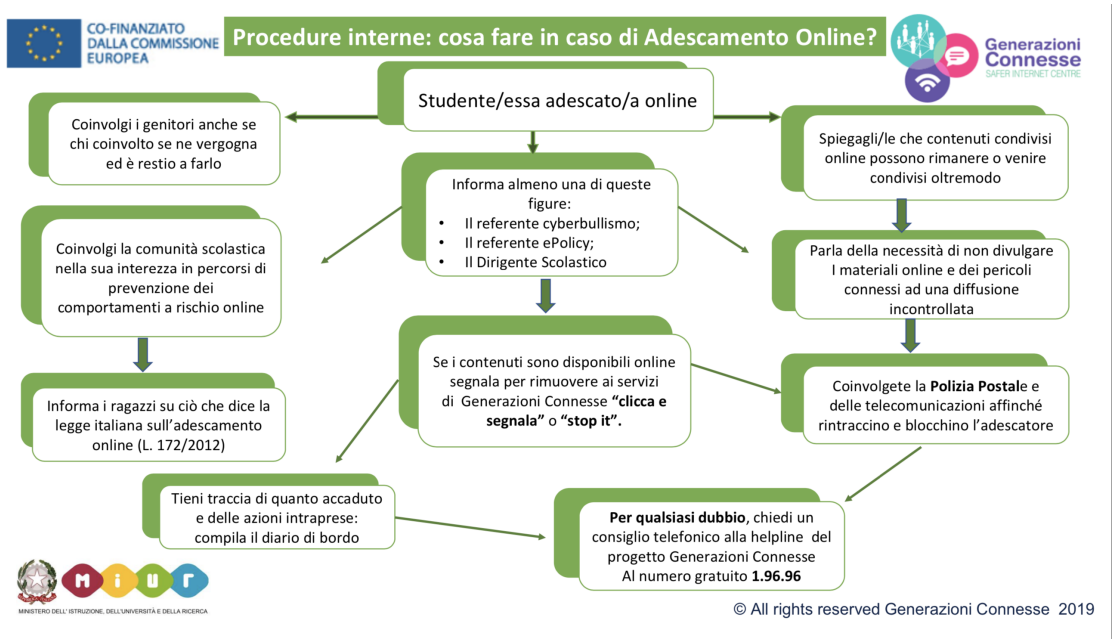
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



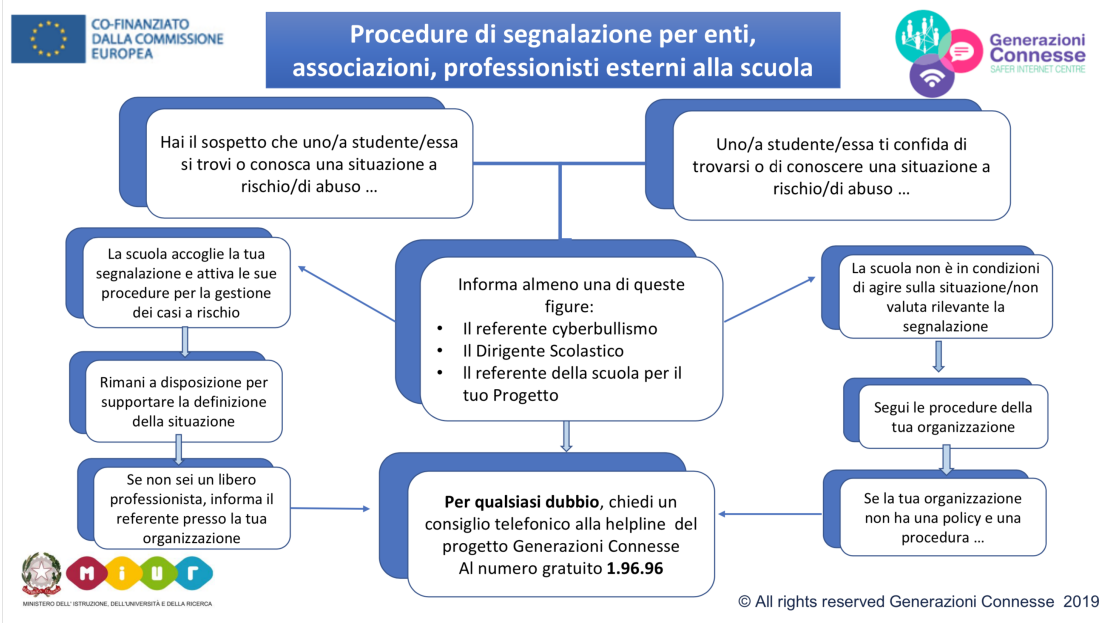
Procedure interne: cosa fare in caso di sexting?



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

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

- coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori e personale ATA, per l'affermazione di un modello di scuola come comunità;

- alleanza educativa tra scuola e famiglia;

- interventi educativi ed azioni di supporto, quale prevenzione per

eventuali comportamenti a rischio;

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

- promozione dell'educazione al rispetto;

- sviluppo del pensiero critico;

- promozione dell'Educazione Civica Digitale.