



Istituto Scolastico
Comprensivo
Luciani
SS. Filippo
e Giacomo



SEGRETERIA
Via III Ottobre, 8 - 63100 Ascoli Piceno
Tel. 0736 43805
E-mail apic82900b@istruzione.it
PEC apic82900b@pec.istruzione.it



Documento di ePolicy

Capitolo 1 - Introduzione al documento di e-Policy

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 curriculum

1. Curriculum 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.

L'ePolicy consente alla nostra scuola di creare un programma **strutturato di formazione e prevenzione** per tutti gli utenti e di elaborare strategie condivise, chiare ed efficaci per la **segnalazione** delle situazioni a rischio.

L'uso delle tecnologie è promosso dal nostro istituto quale efficace strumento per una didattica integrata e inclusiva. Pertanto, l'utilizzo consapevole delle TIC risulta fondamentale per accedere in **sicurezza** agli ambienti didattici e culturali offerti dal web.

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

- individua un referente ed i componenti del team (2 docenti della primaria, 2 della secondaria compreso il referente e la psicologa del centro d'ascolto dell'ISC) del bullismo e cyberbullismo;
- coinvolge, nella prevenzione e contrasto al fenomeno del bullismo, tutte le componenti della comunità scolastica, particolarmente quelle che operano nell'area dell'informatica, partendo dall'utilizzo sicuro di Internet a scuola;
- prevede all'interno del PTOF corsi di aggiornamento e formazione in materia di prevenzione dei fenomeni di bullismo e cyberbullismo, rivolti al personale docente ed Ata;
- promuove sistematicamente azioni di sensibilizzazione dei fenomeni del bullismo e cyberbullismo nel territorio in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo alunni, docenti, genitori ed esperti; favorisce
- la discussione all'interno della scuola, attraverso i vari organi collegiali, creando i presupposti di regole condivise di comportamento per il contrasto e prevenzione dei fenomeni di bullismo e cyberbullismo;

- prevede azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all'esercizio di una cittadinanza digitale consapevole.

Ha la responsabilità di gestire ed intervenire immediatamente nei casi gravi di bullismo, cyberbullismo ed uso improprio del digitale.

IL REFERENTE DEL BULLISMO E CYBERBULLISMO

- si forma e si aggiorna su temi inerenti i bullismi e i rischi connessi all'uso non consapevole del web;
- promuove la conoscenza e la consapevolezza del bullismo e del cyber-bullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale;
- coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale, anche con eventuale affiancamento di genitori e studenti;
- si rivolge a partner esterni alla scuola, quali servizi sociali e sanitari, aziende del privato sociale, forze di polizia,... per realizzare un progetto di prevenzione;
- cura rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet la "Safer Internet Day".

IL DOCENTE

- si forma e si aggiorna su temi inerenti il bullismo e i rischi connessi all'uso non consapevole del web;
- intraprende azioni congruenti con l'utenza del proprio ordine di scuola, tenuto conto che l'istruzione ha un ruolo fondamentale sia nell'acquisizione e rispetto delle norme relative alla convivenza civile, sia nella trasmissione dei valori legati ad un uso responsabile di internet;
- valorizza nell'attività didattica modalità di lavoro di tipo cooperativo e spazi di riflessione adeguati al livello di età degli alunni.

Ha il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso anche online che veda coinvolti gli studenti.

I GENITORI

- partecipano attivamente alle azioni di formazione/informazione, istituite dalle scuole, sui comportamenti sintomatici del bullismo e del cyberbullismo;
- sono attenti ai comportamenti dei propri figli;
- vigilano sull'uso delle tecnologie da parte dei ragazzi, con particolare attenzione ai tempi, alle modalità, agli atteggiamenti conseguenti (i genitori dovrebbero allertarsi se uno studente, dopo l'uso di internet o del proprio telefonino, mostra stati depressivi, ansiosi o paura);
- accettano e condividono le azioni messe in campo dalla scuola e collaborano secondo le modalità previste dal Patto di corresponsabilità;
- accettano e condividono il codice di comportamento dello studente;

- accettano e condividono le sanzioni previste dal regolamento d'istituto nei casi di bullismo, cyberbullismo e navigazione on-line a rischio.

GLI ALUNNI

- sono coinvolti nella progettazione e nella realizzazione delle iniziative scolastiche, al fine di favorire un miglioramento del clima relazionale;
- imparano le regole basilari, per rispettare gli altri, quando sono connessi alla rete, facendo attenzione alle comunicazioni che inviano;
- non possono, durante le attività didattiche o comunque all'interno della scuola, acquisire – mediante telefonini cellulari o altri dispositivi elettronici - immagini, filmati o registrazioni vocali, se non per finalità didattiche, previo consenso del docente. La divulgazione del materiale acquisito all'interno dell'istituto è utilizzabile solo per fini esclusivamente personali di studio o documentazione, e comunque nel rispetto del diritto alla riservatezza di tutti;
- durante le lezioni o le attività didattiche in genere non possono usare cellulari, giochi elettronici e riproduttori di musica, se non per finalità didattiche, previo consenso del docente.

ATA – PERSONALE AUSILIARIO E AMMINISTRATIVO

- si forma e si aggiorna su temi inerenti i bullismi e i rischi connessi all'uso non consapevole del web (ausiliari e pers. amministrativo);
- collabora con i docenti alla sorveglianza degli alunni (ausiliari);
- segnala eventuali comportamenti a rischio (ausiliari);
- si forma e si aggiorna sulle leggi inerenti il trattamento dei dati sensibili e la tutela della privacy e le applica all'interno delle procedure amministrative (pers. amministrativo)

TEAM ANTIBULLISMO

- si forma e si aggiorna su temi inerenti i bullismi e i rischi connessi all'uso non consapevole del web
- gestisce la piattaforma d'istituto nella tutela della sicurezza degli alunni e del personale della scuola;
- propone attività di formazione sull'uso consapevole delle piattaforme e dei dispositivi della scuola e in uso da parte degli alunni.

PERSONALE ESTERNO (enti e associazioni educative, forze dell'ordine, servizi sociali, addetti al servizio mensa e al pre e post scuola, personale del trasporto,)

- segnalano eventuali situazioni a rischio, coerentemente con le procedure scolastiche;
- si attengono alle linee guida della e-Policy di istituto durante l'erogazione dei servizi;
- propongono attività e/o progetti di prevenzione alle prevaricazioni e ai rischi del web.

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).

All'interno del nostro Istituto collaborano con il personale scolastico le seguenti figure:

EDUCATORI PROFESSIONALI, in compresenza con i docenti per la gestione degli alunni con disabilità;

ESPERTI ESTERNI COINVOLTI IN ATTIVITA' PROGETTUALI;

FIGURE DI RIFERIMENTO PER LA GESTIONE DEI SERVIZI DI PRE E POST SCUOLA all'interno dei locali scolastici e durante il trasporto;

Tutti gli attori sopra citati sono tenuti a conoscere e rispettare le linee guida dell'ePolicy dell'Istituto e a segnalare eventuali comportamenti non adeguati.

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/le 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.

Il documento di ePolicy viene condiviso con la comunità educante, oltre che attraverso le modalità sopradescritte, anche mediante l'organizzazione di una serata informativa che coinvolga le parti adulte della scuola, dai docenti, ai genitori, agli attori tutti che collaborano con essa e che possano essere portatori consapevoli dei contenuti del documento.

Gli **alunni**, a loro volta, vengono informati sui seguenti aspetti:

- controllo dell'utilizzo di internet da parte degli alunni e dei dispositivi in uso;
- esplicitazione e condivisione della *Netiquette*, anche attraverso lavori di peer to peer;
- esposizione in ogni aula di cartellonistica riguardante la sicurezza online e il buon uso del web.

I **docenti** vengono formati sui contenuti della ePolicy e vengono chiamati:

- ad un'adeguata informazione/formazione sull'uso sicuro e responsabile di Internet;
- a condividere negli organi collegiali la linea di condotta della scuola in materia di sicurezza e di buone pratiche nell'utilizzo dei dispositivi e del web.

I **genitori** saranno coinvolti dalla scuola al fine di

- collaborare nel perseguimento della sicurezza nell'uso delle TIC e di Internet;
- ricevere suggerimenti e indicazioni per l'autoformazione e riguardo alle procedure stabilite dalla scuola per la segnalazione delle situazioni a rischio;
- ottenere aggiornamenti sull'e-policy e sulle attività formative e progettuali, tramite la consultazione del sito dell'Istituto.

1.5 - Gestione delle infrazioni alla e-Policy

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.

La scuola predispone un piano di gestione delle infrazioni. Si riportano pertanto i principali rischi legati ad un uso non consapevole delle TIC e le procedure di segnalazione e presa in carico delle stesse.

Tra i principali rischi connessi all'uso scorretto delle TIC si citano in particolare:

- **condivisione online di immagini o video** di docenti e/o compagni che li ritraggono senza il loro consenso e quello della famiglia con scopo denigratorio e offensivo;
- condivisione di scatti intimi e a scopo sessuale (**sexting**);
- condivisione di dati personali (**privacy**);
- **adescamento online**;
- l'invio di immagini o video volti all'esclusione e **isolamento** di compagni/e;
- partecipazione a gruppi e **chat online che fomentano all'odio** o alla denigrazione.

La scuola predispone una procedura strutturata per la segnalazione delle situazioni a rischio, utilizzando una modulistica ad hoc, costruita a partire da alcuni documenti tratti dalla Piattaforma Elisa e personalizzati a seconda degli ordini di scuola del nostro Istituto.

Il capitolo 5 riporta dettagliatamente la procedura di segnalazione adottata dalla nostra scuola e le azioni educative da intraprendere e/o di denuncia alle autorità.

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.

Per il Regolamento di Istituto e il Patto di Corresponsabilità, aggiornati con specifici riferimenti all'e-Policy e in coerenza con le linee guida del MIUR, **si rimanda ai documenti presenti sul sito dell'Istituto www.isclucianiap.edu.it**

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Capitolo 2 - Formazione e curriculum

2.1. Curriculum 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 curriculum digitale.

Le **competenze digitali** rientrano tra le otto competenze chiave che la Comunità Europea ha individuato per il pieno sviluppo della cittadinanza (Raccomandazioni del Parlamento Europeo e del Consiglio “Le competenze chiave per l’apprendimento permanente”, 2006).

La competenza digitale è una competenza trasversale, quindi tutti i docenti sono chiamati a promuoverla e a favorirla all’interno della propria programmazione educativo-didattica.

L’obiettivo è quello di rispondere ai bisogni di conoscenza consapevole, di espressione e di comunicazione dei ragazzi affinché sappiano riflettere e attribuire senso alla loro esperienza tecnologica. Si promuove l’uso non passivizzante della tecnologia, finalizzato dunque ad un’esperienza tecnologica consapevole.

In quest’ambito si seguono le indicazioni contenute nel PNSD (azione 14), in cui si

individuano alcuni framework di riferimento per la definizione e lo sviluppo delle competenze digitali, tra cui il DIGCOMP, che prevede 21 competenze.

Il nostro Istituto si impegna a lavorare ad un **Curricolo Digitale verticale**, all'interno del **curricolo verticale di educazione civica**, ossia un percorso didattico progettato per sviluppare competenze digitali, dal quale emergano le competenze in uscita da raggiungere al termine dei tre ordini di scuola di nostracompetenza (Infanzia, primaria e Secondaria I grado).

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.

L'Istituto ha aderito alla formazione promossa dal MIUR attraverso le piattaforme di Generazioni Connesse e Piattaforma Elisa, indirizzandola ai docenti del team bullismo e cyberbullismo.

Sono state attivate iniziative di formazione facendo ricorso a soggetti esterni, ad associazioni territoriali e a personale interno alla scuola che ha acquisito competenze su innovazione didattica e rischi connessi alla rete.

Il collegio dei docenti è stato informato dal gruppo di lavoro per l'e-Policy rispetto alle attività che si stanno progettando.

Il percorso della formazione specifica dei docenti sull'uso delle TIC nella didattica deve diventare un processo permanente, che preveda anche momenti di autoaggiornamento, di formazione personale o collettiva.

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 (team digitale, gruppo antibullismo 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.

Coerentemente con quanto previsto dal PNSD, l'Istituto si avvale delle *funzioni strumentali dell'Area 2*, referenti per i sussidi ed il digitale, insieme al *Gruppo digitale* dell'Istituto che coordinano la diffusione dell'innovazione digitale e collaborano con tutti i soggetti che possono contribuire alla realizzazione degli obiettivi del Piano.

Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di internet prevede momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

Si prevede, inoltre, la promozione di attività formative interne avvalendosi di risorse interne e/o esterne.

Il docente referente partecipa a specifiche iniziative di formazione dedicate alla prevenzione e contrasto del bullismo e cyberbullismo.

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

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle

tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

La scuola organizza incontri aperti alle famiglie e ai docenti in orario extrascolastico, e agli studenti in orario scolastico, con enti esterni per sensibilizzare tutte le figure sul tema della sicurezza online.

Si tratta di incontri che offrono un'occasione di confronto e discussione sui rischi rappresentati dall'uso di cellulari e social in mancanza di una formazione adeguata su tali temi.

Si aggiorna periodicamente il sito scolastico rendendo note le attività di formazione proposte, creando una sezione dedicata al documento e-Policy e ai materiali inerenti rischi e potenzialità del web.

2.5 - Il nostro piano d'azione

Azioni da svolgere entro un'annualità scolastica 2021/2022

1. Organizzare un evento rivolto a **tutto il personale scolastico**, volto a presentare il progetto Generazioni Connesse, il documento e-Policy e le principali emergenze sul tema del bullismo in ambito scolastico e sociale con particolare riferimento all'ambiente social-media.
2. Organizzare un evento rivolto ai **genitori** degli alunni dell'ISC volto a trattare le principali emergenze sul tema del bullismo in ambito scolastico e sociale con particolare riferimento all'ambiente social-media.
3. Organizzare uno o più eventi rivolti agli **alunni** dell'ISC volti a trattare le principali emergenze sul tema del bullismo in ambito scolastico e sociale con particolare riferimento all'ambiente social-media.

Azioni da svolgere nei prossimi 3 anni

1. Effettuare un'analisi del fabbisogno formativo del corpo docente, genitori e degli studenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
2. Organizzare eventi di presentazione del progetto Generazioni Connesse rivolto al personale scolastico, genitori e studenti nonché di formazione/informazione sull'uso consapevole dei social-media e cittadinanza digitale
3. Promuovere attività di monitoraggio del fenomeno in ambito scolastico e sociale

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.

Allegato 1 – Autorizzazione ai diritti di immagine

Allegato 2 - Autorizzazione accesso personale esterno alla scuola per effettuare foto-filmati e successive rielaborazioni necessarie per la stampa e/o produzione di cd-rom, video, altro finalizzate alla condivisione del materiale raccolto con tutti i genitori della/e classe/i- sezione/i o alla partecipazione progetti, eventi e concorsi.

Allegato 3 - Realizzazione di foto-filmati e successive rielaborazioni necessarie per la stampa e/o produzione di cd-rom, video, altro finalizzate alla condivisione del materiale con tutti i genitori della/e classe/i-sezione/i o alla partecipazione a progetti, eventi e concorsi.

Allegato 4 - Conferimento Incarico Responsabile Esterno del Trattamento Dati

3.2 - Accesso ad Internet

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

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

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

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

La scuola garantisce ai docenti la possibilità di accedere a internet attraverso una buona infrastruttura di rete in grado di supportare il traffico dati generato da un numero elevato di utenti.

La connessione, in fibra ottica e cablata per il plesso della scuola secondaria, è dotata di firewall, mentre negli altri plessi l'accesso è tramite Wifi. Interventi, atti a migliorare la performance e sicurezza di rete, sono stati previsti già per l'A.S. 2021/2022 oltre ai periodici interventi di manutenzione e verifica. Altre verifiche possono essere effettuate su segnalazione degli utenti.

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.

Il nostro istituto adotta per tutto il personale e gli studenti la Google Edu Suite, una piattaforma integrata a marchio Google che consente di comunicare e di gestire contenuti digitali con grande semplicità e flessibilità. Le apps di Google garantiscono sicurezza e privacy, connessione e interoperabilità, comunicazione facilitata tra docenti e studenti.

Tutti gli studenti hanno accesso ad una serie di servizi, tra i quali:

- e-mail personale con spazio di archiviazione illimitato;
- Google Drive, che permette di archiviare online tutti i tipi di file, senza limiti di spazio;
- Google Classroom, per avere una classe virtuale nella quale lavorare attivamente e ricevere materiale aggiuntivo da parte degli insegnanti.

Gli studenti ed i genitori devono tuttavia sapere, nel momento in cui ricevono le credenziali di accesso, che i servizi offerti sono **ESCLUSIVAMENTE** per utilizzo scolastico e didattico.

L'utilizzo della Google Suite è indispensabile per realizzare l'azione didattica programmata nel PTOF di Istituto. Nel momento in cui gli account degli studenti vengono creati e attivati, i genitori sono responsabili della vigilanza sull'utilizzo degli account scolastici a casa e sui dispositivi personali degli studenti, in particolare sull'utilizzo degli account per finalità esclusivamente didattiche e in accordo con i docenti.

La scuola fornisce agli studenti un indirizzo di posta elettronica personale attivo per il tempo di permanenza nell'Istituto: gli studenti dovranno utilizzarlo per accedere alle piattaforme e-learning e tutte le attività ICT della scuola stessa. Lo stesso avviene per gli account di docenti e personale della scuola. Quando possibile, i pc della scuola sono programmati per effettuare gli aggiornamenti periodici sia del software che del Sistema operativo. I docenti sono tenuti a tenere aggiornati e ordinati i pc di classe, anche cancellando con frequenza dati sensibili e documenti/software superflui. Essi sono inoltre invitati a non salvare su pc collocati in aree comuni (es. aula informatica) file personali o contenenti dati personali degli alunni.

La scuola garantisce formazione adeguata allo staff, incluso il corpo docenti sulla gestione dei dispositivi e sulle regole basilari sulla sicurezza.

Policy sulle password: le password devono essere forti e non facilmente identificabili, non devono essere memorizzate nei dispositivi scolastici e non devono essere condivise con nessuno.

Strumenti di comunicazione online che possono essere utilizzati a scuola:

COMUNICAZIONE ESTERNA: lo strumento utilizzato dalla scuola sia al fine di valorizzare e promuovere le attività portate avanti dall'Istituto, sia per far circolare all'interno della scuola informazioni di servizio o contenuti importanti fra i diversi attori scolastici è la Bachecca del Registro Elettronico e il sito web dell'ISC. La comunicazione esterna dell'Istituto può essere progettata ed implementata anche con il supporto degli studenti opportunamente guidati, che possono produrre contenuti multimediali da diffondere.

COMUNICAZIONE INTERNA: con lo scopo di facilitare e rendere più partecipata la didattica e la comunicazione a scuola, vengono utilizzati: registro elettronico, email istituzionale, app della piattaforma Google Suite.

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, è importante ricordare quello che si può definire "diritto alla disconnessione" (art. 22 - Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola del CCNL 2016/2018).

Per le chat informali fra colleghi, o fra docenti e genitori, non esiste una vera e propria regolamentazione, e per tale ragione si stabiliscono le seguenti regole condivise sull'uso:

- 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;
- 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.

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);
- circolari e comunicazione varie (comunicazioni di classe, comunicazioni personali).

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le 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.

Nel Piano Nazionale Scuola Digitale emanato dal Miur con la Legge 107 del 2015 leggiamo: “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. Attualmente l’istituto non prevede il BYOD con i dispositivi mobili, anche sulla base delle norme esistenti relative all’impossibilità di un minore di 14 anni di avere un proprio indirizzo email. In occasione della didattica a distanza sono stati forniti invece device dall’istituto agli studenti. È previsto l’utilizzo di apparecchiature personali in situazioni particolari (alunni con difficoltà). Per il resto l’istituto mette a disposizione, allo stato attuale, tutti gli apparecchi necessari per la didattica. In caso di ulteriore necessità, l’istituto si impegna a regolamentare l’utilizzo dei dispositivi personali. I docenti possono ovviamente utilizzare i propri dispositivi, collegandoli alla rete WiFi o LAN di istituto, con le modalità stabilite anno per anno dai dispositivi dirigenziali, e a soli fini didattici, sia in aula che per le attività correlate.

In merito all’utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l’attività didattica, si ricorda che quando autorizzato dal docente, 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”).

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.

In virtù della normativa vigente posta a tutela della privacy, è fatto divieto di utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire, divulgare e/o pubblicare immagini, filmati o registrazioni vocali senza il consenso esplicitamente espresso in forma scritta dagli interessati o i loro tutori (nel caso di minori). 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.

3.5 Il nostro piano d'azione

1. Effettuare un'analisi sull'utilizzo dei dispositivi tecnologici presenti a scuola e fruibili da parte degli studenti e dei docenti
2. Organizzare uno o più eventi o attività volti a formare il personale scolastico e genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali (cybersecurity)
3. Effettuare proposte per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Per tutti i rischi online descritti in questa sezione, il nostro Istituto adotta particolari metodologie didattico-educative volte a rinforzare le **life skills** degli alunni e di conseguenza a favorire la **prevenzione** e **sensibilizzazione** negli utenti.

In particolare, si propongono le seguenti modalità:

- role playing e attività di tipo teatrale;
- realizzazione di spot sociali e pubblicità progresso sulle tematiche in oggetto;
- video clip a tema;

- attività di peer to peer per la sensibilizzazione degli alunni più giovani da parte di quelli più grandi;
 - attività di Debate;
 - attività ludiche e giochi da tavolo studiati ad hoc per affrontare e prevenire le situazioni a rischio;
 - cineforum: visione strutturata e guidata di film inserenti il tema delle prevaricazioni online.
-

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).

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.

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.

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 medialti 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.

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).

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 [Azzurro](#) e "STOP-IT" di [Save the Children](#)

4.8 – Il nostro piano d'azione

1. Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.
2. 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/le studenti/studentesse.
3. Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.
4. 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.
5. 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 minorenni 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.

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 ed alle 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](tel:19696).

Il docente che ha il sospetto o che possiede evidenza certa di una situazione di rischio avrà cura, in linea generale, di:

- 1) compilare la SCHEDA DI SEGNALAZIONE avendo cura di riportare i fatti con precisione e i nomi di tutti gli attori coinvolti;
- 2) informare il Dirigente Scolastico e il Referente per il contrasto ai bullismi per stabilire la linea di azione;
- 3) informare il/i CDC/TEAM coinvolto/i;
- 4) MONITORARE e OSSERVARE la situazione avendo cura di integrare la segnalazione se necessario;
- 5) informare le famiglie coinvolte;
- 6) incontrare gli studenti coinvolti;
- 7) contattare eventuali enti esterni, laddove le competenze vadano oltre quelle scolastiche (forze dell'ordine, servizi sociali...).

Si precisa che ognuno di questi punti va condiviso con il Dirigente Scolastico e deve essere attivato o meno sulla base dell'analisi della singola situazione. La celerità dell'intervento garantisce inoltre che le dinamiche di prevaricazione si cronicizzino.

PER STUDENTI E STUDENTESSE

Gli studenti possono comunicare in qualunque momento con il coordinatore della propria classe e con il referente per la prevenzione ai bullismi.

Si predispongono strumenti quali il box per la segnalazione anonima, la mail di istituto dei docenti di riferimento, i colloqui individuali con la psicologa (sportello psicologico).

Inoltre, è attiva la possibilità di organizzare con la psicologa incontri ad hoc sul gruppo classe per prevenire e/o affrontare situazioni di malessere e a rischio.

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.

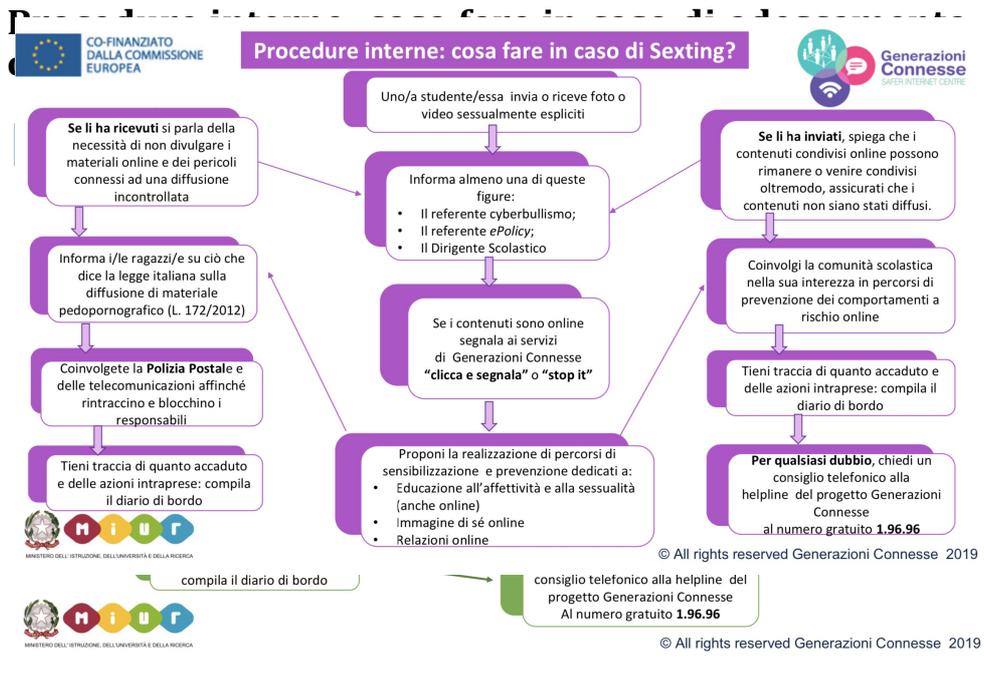
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell’infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

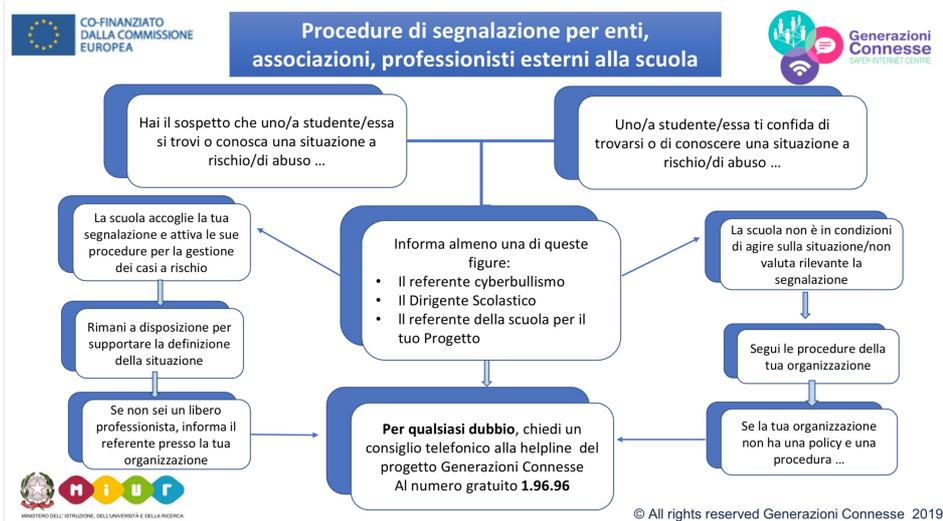
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



Procedure interne: cosa fare in caso di sexting?



Procedure 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](#)

La scuola si impegna a prendere in carico le situazioni a rischio, segnalando i fatti avvenuti mediante l'utilizzo delle procedure sopra citate, al fine di non trascurare alcun attore coinvolto o figura/ente di riferimento.

Il nostro piano d'azioni

A partire dall'anno scolastico 2021/2022, la scuola adotta le procedure indicate per la segnalazione delle situazioni a rischio, al fine di prevenire e sensibilizzare tutti gli attori coinvolti.

Al Dirigente scolastico

I.S.C. "Luciani SS. Filippo e Giacomo"- AP

Al/la docente _____

I.S.C. "Luciani SS. Filippo e Giacomo"- AP

Autorizzazione ai diritti di immagine plesso _____ sez. _____

(condivisione del materiale raccolto con i genitori della/e classe/i-sezione/i del plesso - partecipazione a progetto, evento o concorso)

Il Sottoscritto genitore/tutore dell'alunno/a _____ frequentante la classe/sez _____ plesso _____, anno scolastico _____, dichiara di aver preso visione dell'informativa trattamento dati personali applicata dall'Istituto Scolastico (disponibile all'albo online dell'Istituto) art. 13 del Regolamento Europeo 2016/679 e

autorizza

- il/la Sig./Sig.ra _____, ruolo _____
(rappresentante di classe/fotografo/genitore di un alunno della classe,altro)
- il/i docente/i _____, ruolo _____
(nome cognome/referente di plesso/di sezione plesso)

a titolo gratuito, senza limiti di tempo, luogo e mezzo, anche ai sensi degli artt. 10 e 320 cod. civ. e degli artt. 96 e 97 legge 22.4.1941 n. 633, ad effettuare foto e filmato del/lla proprio/a figlio/a in occasione dell'attività scolastica _____ (tipo di attività) che avrà luogo il _____ (data/e-periodo) per successive rielaborazioni necessarie alla stampa e/o produzione di un cd-rom/video/altro finalizzate alla:

condivisione del materiale raccolto con tutti i genitori della/e classe/i-sezione/i del plesso

I genitori potranno utilizzare il materiale ricevuto per uso strettamente personale. Per la diffusione dovranno personalmente e preventivamente chiedere autorizzazione dalle persone ritratte nelle foto/video o dai loro referenti genitoriali.

partecipazione al Progetto e/o Concorso e/o Evento _____ (titolo dell'iniziativa)

data _____

Firma * _____

*Alla luce delle disposizioni del codice civile in materia di filiazione, qualora l'autorizzazione sia firmata da un solo genitore, si intende che la stessa sia stata condivisa con l'altro.

Si invita a leggere, sul sito web dell'Istituto i chiarimenti pubblicati sulle norme di comportamento per la tutela della privacy degli alunni in occasione di gite, recite scolastiche, partecipazione ad eventi. Si fa presente che il consenso può essere revocato in qualsiasi momento inviando la richiesta al Dirigente Scolastico (Titolare del Trattamento).



I.S.C. "Luciani – SS. Filippo e Giacomo"

Con sezioni ad indirizzo musicale

Via 3 Ottobre, 8/C – 63100 Ascoli Piceno – Tel. 0736.43805 – Fax. 0736.44544 – Cod. Fisc. 92053530447
Mail: apic82900b@istruzione.it – Pec: apic82900b@pec.istruzione.it – CM: APIC82900B – Web: isclucianap.edu.it



AL docente *richiedente*

SUA EMAIL

Al/la Sig./Sig.ra *FIGURA ESTERNA*

SUA EMAIL

OGGETTO: autorizzazione accesso personale esterno alla scuola per effettuare foto-filmati e successive rielaborazioni necessarie per la stampa e/o produzione di cd-rom, video, altro finalizzate alla condivisione del materiale raccolto con tutti i genitori della/e classe/i-sezione/i o alla partecipazione progetti, eventi e concorsi.

In rif. alla richiesta prot. N^ _____ si autorizza l'accesso della/e figura/e delegata/e _____ (riportare estremi e qualifica) presso _____ (riportare luogo) in occasione dell'attività: _____ che avrà luogo nella/e data/e _____ per effettuare foto/ filmati e successive rielaborazioni necessarie per stampa e/o produzione di un cd-rom, video, altro finalizzate alla:

condivisione del materiale raccolto con tutti i genitori della/e classe/i-sezione/i _____ del plesso _____

partecipazione al Progetto e/o Concorso e/o Evento _____ (titolo dell'iniziativa)

A tal proposito si allega il l'incarico Responsabile ESTERNO al trattamento dati che il/la Sig./ra _____ (figura esterna autorizzata) dovrà restituire compilato al docente referente prima dello svolgimento dell'intervento.

I dati della/e figura/e esterna/e impegnata/e nell'attività saranno oggetto di trattamento ai sensi del Regolamento UE 2016/679 e D. Lgs. 196/03 come modificato dal D. Lgs.101/18. L'informativa specifica è consultabile all'albo online dell'Istituto. Per quanto concerne l'igiene, la sicurezza e la salute sui luoghi di lavoro, potranno essere richieste al coordinatore di plesso, le informazioni e quanto previsto per la propria ed altrui tutela nella struttura in cui si andrà ad operare.

Distinti saluti.

LA DIRIGENTE SCOLASTICA

Dott.ssa Elvia Cimica

Allegato: incarico Responsabile ESTERNO al trattamento dati (Modello D privacy)



Ai docenti ed al personale di segreteria
I.S.C. "Luciani SS. Filippo e Giacomo -AP
BACHECHE DIGITALI DI RIFERIMENTO

Oggetto: PRIVACY A.S. 2020/21 –realizzazione di foto-filmati e successive rielaborazioni necessarie per la stampa e/o produzione di cd-rom, video, altro finalizzate alla condivisione del materiale con tutti i genitori della/e classe/i-sezione/i o alla partecipazione a progetti, eventi e concorsi.

Con la presente si comunicano le indicazioni operative in merito a quanto in oggetto.

1- REALIZZAZIONE DA PARTE DEL PERSONALE INTERNO

I docenti potranno procedere a quanto in oggetto sulla base e nel rispetto dell'incarico già assunto in qualità di Responsabili INTERNI al trattamento dati, attenendosi alle disposizioni normative in essere che prevedono la preventiva raccolta delle necessarie autorizzazioni da parte dei soggetti ritratti o, se minori, da parte dei loro referenti genitoriali (**Mod. C privacy**)

2- REALIZZAZIONE DA PARTE DEL PERSONALE ESTERNO

La procedura prevede:

- 1- raccolta da parte del docente referente delle necessarie autorizzazioni dei soggetti ritratti o, se minori, dei loro referenti genitoriali (**Mod. C privacy**); le autorizzazioni raccolte non dovranno essere consegnate a scuola ma conservate dal docente richiedente che, in caso di necessità, potrà esibirle per documentare quanto dichiarato nella richiesta;
- 2- richiesta di autorizzazione alla scuola da parte del docente referente, da presentare con adeguato anticipo; non potranno essere accettate richieste formalizzate in modo differente vista l'autodichiarazione che dovrà essere formalizzata nel modulo (**Mod. A privacy** presente su *Nuvola modulistica*- PRIVACY - Richiesta accesso figura esterna per foto e video)
- 3- a cura dell'ufficio protocollo: predisposizione ed invio della lettera di autorizzazione (**Mod. B privacy**) con allegato *l'incarico Responsabile ESTERNO al trattamento dati* (**Mod. D privacy**) - copia conforme segnata e firmata - per la figura esterna che effettuerà l'intervento.

LA DIRIGENTE SCOLASTICA
Dott.ssa Elvia Cimica

Allegati: Mod. A privacy
Mod. B privacy
Mod. C privacy
Mod. D privacy

