Documento di ePolicy

COIC82100L

ISTITUTO COMPRENSIVO DI TURATE

VIA GIUSEPPE GARIBALDI 39 - 22078 - TURATE - COMO (CO)

Angela Serena Ildos

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.

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 ha il compito di:

- garantire la sicurezza, anche on-line, dei membri della comunità scolastica;
- organizzare per gli insegnanti i necessari corsi di formazione che li supportino nella promozione di una cultura inclusiva, del rispetto dell'altro/a e delle differenze, attraverso l' utilizzo positivo e responsabile delle TIC;
- prevenire le problematiche legate all'uso della rete, in linea con le normative del Miur;
- Intervenire in caso di mancato rispetto delle norme indicate nella Epolicy.

il referente del bullismo/cyberbullismo deve attivarsi per:

- coordinare e promuovere le iniziative necessarie a prevenire e contrastare bullismo e cyberbullismo;
- vigilare sulla corretta applicazione della e-policy e delle linee guida in materia di bullismo e cyberbullismo;
- provvedere periodicamente all' aggiornamento della e-plicy, anche in funzione dell'evoluzione delle tecnologie digitali;
- collaborare con il Dirigente scolastico per l'organizzazione delle attività di informazione-formazione rivolte ad alunni, studenti e personale scolastico, in materia di bullismo,cyberbullismo e cittadinanza digitale;
- organizzare percorsi rieducativi per gli alunni che non hanno rispettato le norme previste dal presente documento;
- intervenire in sostegno delle vittime di bullismo o cyberbullismo, avvalendosi dell'appoggio delle agenzie educative e delle associazioni del territorio, oltre che delle forze dell'ordine nei casi più gravi:

Il Team digitale vigila sul corretto uso delle tecnologie a scuola impegnandosi a:

- pubblicare e diffondere la E-Safety Policy sul sito della scuola;
- monitorare l'utilizzo sicuro delle tecnologie digitali e di internet a scuola, proteggendo i dati personali della comunità scolastica;
- promuovere corsi di formazione per lo sviluppo della "scuola digitale".
- supportare il personale scolastico sia dal punto di vista tecnico, sia in riferimento agli effettivi rischi che si possono affrontare in internet.

Il personale docente ha il compito di:

- stimolare gli alunni ad un uso corretto e consapevole delle tic e della rete;
- integrare le attività curricolari con l'uso delle nuove tecnologie;
- segnalare al Dirigente scolastico qualsiasi problema, violazione o abuso subiti dai loro

studenti;
- suggerire integrazioni e modifiche al documento di e-policy;
- aggiornarsi sulle problematiche legate all'uso improprio delle tic;
- informarsi sulla politica di sicurezza adottata dalla loro scuola.

Il personale ATA ha il compito di:

- collaborare con il DS, il DSGA e i docenti nella prevenzione ed intercettazione di situazioni legate ad un uso scorretto delle nuove tecnologie o alle norme in materia di bullismo e cyberbullismo;
- segnalare al dirigente e al responsabile per il cyberbullismo eventuali infrazioni al regolamentoe-policy;
- adottare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia.

Gli alunni dell'Istituto sono chiamati a collaborare con gli adulti affinchè il presente documento venga rispettato; essi devono:

- approcciarsi all'uso delle nuove tecnologie con responsabilità e maturità;
- essere coscienti che la rete nasconde pericoli e vigilare sulla propria sicurezza, nonchè sull'incolumità dei compagni;
- suggerire modifiche ed integrazioni al documento di e-policy;
- partecipare alle iniziative di aggiornamento e informazione riguardanti le Tic;
- segnalare all'adulto di riferimento eventuali abusi o violenze subite in prima persona o da altri studenti.

I genitori hanno il compito di:

- Accettare il documento di e-policy;
- vigilare sull'uso che i loro figli fanno dei dispositivi tecnologici personali o scolastici;
- collaborare con il personale scolastico per la diffusione di una cultura inclusiva;
- concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati in seguito ad un uso non responsabile o pericoloso delle tecnologie digitali o di internet.

In ultima istanza gli Enti e le agenzie educative del territorio, nel collaborare con la comunità scolastica per progetti ed iniziative volte allintegrazione del curricolo, devono:

- conformarsi al documento di e-policy;
- promuovere l'uso consapevole della rete nel rispetto di una cultura che sostenga il rispetto dell'altro e l'inclusività.

.

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).

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

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

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

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

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

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

1.5 - 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.

In caso di infrazione del documento di e-policy e di episodi lesivi della libertà personale di adulti o studenti, l'intervento della scuola affiancherà alle sanzioni, le azioni educative e formative necessarie al recupero di chi ha utilizzato la rete senza avere la consapevolezza dei danni perpetrati.

I provvedimenti saranno sempre adeguati alla gravità dell'atto commesso e all'età della persona coinvolta.

Condotte sanzionabili:

- utilizzare la rete per interessi privati e personali che esulino dalla didattica;
- diffusione di immagini lesive della libertà altrui;
- condivisione di immagini o video che riguardino soggetti terzi senza il loro permesso;
- utilizzo di audio, video, immagini con lo scopo di denigrare, creare imbarazzo o screditare;
- diffusione di dati personali o sensibili;
- attuare cyberstalking o altre forme di persecuzione e molestia attraverso l'uso delle TIC;

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.

Il gruppo di lavoro che gestisce la e-policy della scuola, in raccordo con il Collegio Docenti, opera al fine di integrare i regolamenti dell'Istituto con il presente documento, proponendo al Consiglio d'Istituto le necessarie modifiche.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti;
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti;
- Organizzare 1 evento di presentazione e conoscenza dell' epolicy rivolto ai genitori;
- Monitorare l'efficacia dell'e-policy ai fini di verifcarne l'adeguatezza alle esigenze dell'Istituto.

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.

L'Istituto sta affrontando in modo condiviso la creazione di un curricolo verticale delle competenze digitali che tenga conto del crescente livello di abilità tecnica degli alunni, nella consapevolezza che tale crescita non sempre si accompagna ad un equivalente aumento di consapevolezza.

Il curricolo è al momento in fase di elaborazione.

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

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

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

La formazione sulle TIC è presente nel Piano della Formazione dei docenti e del personale ATA ed ogni anno si concretizza in corsi di formazione specifici per rispondere ai bisogni formativi rilevati a inizio anno.

2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

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

l'Istituto scolastico ha organizzato per i docenti un corso sul corretto uso della piattaforma Gsuite for Education; inoltre la commissione che si occupa di Educazione alla cittadinanza ha proposto ai colleghi l'utilizzo dei materiali elaborati per l'ed. civica dall'associazione Parole Ostili.

La scuola Primaria ha aderito all'attività "Bambini adescati in rete perchè navigano inconsapevoli. Come tutelarli?" proposta dall'Osservatorio Nazionale Adolescenza Onlus. Il progetto prevede le attività con i ragazzi delle classi quinte e quarte e un corso di formazione sulle tematiche dell'adescamento online per i docenti.

Tra i progetti dell'Istituto, molta importanza ha la l'attività di collaborazione tra le scuole con la quale numerosi Istituti Comprensivi del territorio si aiutano nella gestione delle situazioni di maltrattamento e violenza assistita familiare perpetrati ai danni di minori: "PROGETTO LA RETE Si-Cura" gestito in collaborazione con ASCI.

Nell'anno scolastico 2018-19 la scuola ha aderito al progetto "Be Social Be Different" (all'interno del

progetto N.3 IN RETE SICURI) destinato alle classi 4^, 5^ primaria e prima secondaria.
L'intervento é partito dalla convinzione che la consapevolezza delle possibilità, dei limiti e dei rischi connessi all'utilizzo delle tecnologie in Rete aiuti i ragazzi a crescere e interagire meglio con
la società nel rispetto dei diritti umani e civili e della dignità della loro e dell'altrui persona.
Da tale assunto emerge chiaramente come sia importante assicurare alle nuove generazioni un efficace supporto nella prevenzione di forme di violenza mediatica derivanti da un utilizzo improprio e pericoloso delle tecnologie diffuse quali l'adescamento on-line, il cyberbullismo e il cybercrime.

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.

ISTITUTO COMPRENSIVO DI TURATE

PATTO DI CORRESPONSABILITA' EDUCATIVA (ai sensi del DPR n. 235/07)

La scuola affianca al compito dell'insegnare ad apprendere quello dell'insegnare ad essere, poiché tra le sue finalità c'è quella di educare alla convivenza civile, ma può svolgere questo compito solo con una fattiva collaborazione con la famiglia. I rapporti devono essere costanti e sempre rispettosi dei ruoli.

La scuola e la famiglia cooperano per raggiungere comuni finalità educative e condividere quei valori che fanno sentire gli alunni membri di una comunità vera.

Con queste premesse si stipula il seguente patto di corresponsabilità, che le famiglie sono invitate a leggere con attenzione insieme ai ragazzi per acquisire consapevolezza dei diritti e doveri di ciascuno.

	La scuola si impegna a:	La famiglia si impegna a:	L'alunno/a si impegna a:
Offerta formativa	• Garantire un piano dell'offerta formativa basato su progetti e iniziative volte a promuovere il benessere e il successo dell'alunno, la sua valorizzazione come persona, la sua realizzazione umana e culturale. • Organizzare e condividere interventi di formazione e prevenzione in materia di bullismo/cyberbullismo rivolti al personale, agli studenti e alle famiglie.	• Prendere visione del piano formativo e del patto educativo di corresponsabilità, condividerlo, discuterlo con i propri figli, assumendosi la responsabilità di quanto sottoscritto. • Partecipare alle iniziative di formazione/informazione organizzate dalla scuola o da enti esterni sul cyberbullismo.	• Condividere con gli insegnanti e la famiglia la lettura del piano formativo e del patto di corresponsabilità e partecipare attivamente ai progetti e alle iniziative proposte. • Partecipare in modo attivo agli interventi proposti dalla scuola per affrontare e gestire episodi di bullismo e cyberbullismo.
Relazione / Collaborazione	• Creare un clima sereno in cui stimolare il dialogo e la discussione, favorendo la conoscenza reciproca, l'integrazione, l'accoglienza, il rispetto di sé e dell'altro. • Promuovere le potenzialità, i comportamenti ispirati alla partecipazione, alla gratuità, al senso di cittadinanza.	• Condividere con i docenti linee educative comuni in modo da consentire la continuità nell' azione formativa dei propri figli.	• Mantenere costantemente un comportamento positivo e corretto. • Instaurare rapporti di collaborazione e di rispetto nei confronti di compagni, docenti e personale della scuola. • Rispettare l'ambiente scolastico avendo cura di spazi, arredi e attrezzature.

Partecipazione	**• Ascoltare e coinvolgere gli alunni e le famiglie nell' assunzione di responsabilità rispetto a quanto espresso nelle proposte formative.** **• Comunicare costantemente con le famiglie, informandole sull'andamento didattico – disciplinare degli alunni.** **• Fare rispettare le norme di comportamento e i regolamenti.** **• Prendere adeguati provvedimenti disciplinari in caso di infrazioni.** **• Segnalare ai genitori e alle autorità competenti i casi di bullismo/cyberbullismo di cui viene a conoscenza.** **• Gestire le situazioni problematiche di bullismo/cyberbullismo sia attraverso interventi educativi, sia attraverso i necessari provvedimenti disciplinari.**	**• Collaborare attivamente per mezzo degli strumenti messi a disposizione dall'istituzione scolastica, informandosi costantemente sul percorso educativo – didattico dei figli.** **• Prendere visione e firmare tutte le comunicazioni provenienti dalla scuola.** **• Favorire un'assidua frequenza dei propri figli alle lezioni, evitando il più possibile assenze e ritardi.** **• Discutere con i figli le eventuali decisioni e i provvedimenti disciplinari, stimolando una riflessione su quanto accaduto.** **• Stabilire regole per l'utilizzo dei social network da parte dei propri figli e controllarne le attività online.** **• Segnalare tempestivamente alla scuola e/o alle autorità competenti episodi di cyberbullismo di cui si viene a conoscenza, anche se messi in atto al di fuori dell'orario scolastico.**	**• Essere puntuale e frequentare regolarmente le lezioni** **• Impegnarsi con costanza nello studio** **• Partecipare in modo positivo alle attività scolastiche.** **• Riferire in famiglia le comunicazioni provenienti dalla scuola.** **• Non rendersi protagonisti di episodi di bullismo o cyber bullismo e segnalare a genitori e/o docenti episodi di cui è vittima o testimone.** **• Dissociarsi in modo esplicito sui social network da episodi di cyberbullismo invitando gli autori a desistere da tali comportamenti.**

Il Dirigente Scolastico **Firma dei**

Prof. Angela Serena Ildos **GENITORI**

Firma dell'alunno/a

Il nostro piano d'azioni

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali per integrare la didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali per integrare la didattica.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

personali.

ISTITUTO COMPRENSIVO DI TURATE

INFORMATIVA PRIVACY AGLI ALLIEVI

Redatta ai sensi degli Artt. da 13 a 15 del Regolamento U.E. 2016/679 (G.D.P.R.)
Prima che Lei ci fornisca i dati personali che La riguardano, in applicazione del Regolamento Europeo sulla protezione dei dati personali, è opportuno che prenda visione di una serie di informazioni che La possono aiutare a comprendere le motivazioni per le quali i Suoi dati verranno trattati e quali sono i diritti che potrà esercitare rispetto a questo trattamento.

- Per quale finalità saranno trattati i miei dati personali ?

Il trattamento dei dati personali necessari, pertinenti e non eccedenti, conseguente all'iscrizione dell'allievo all'Istituto scolastico avverrà allo scopo di costituire, perfezionare e mantenere il rapporto con
l'Istituto stesso per il perseguimento delle finalità istituzionali dell'Istituto nonché del Ministero dell'Istruzione dell'Università e della Ricerca (M.I.U.R.) previste da leggi, regolamenti e dalla normativa
comunitaria, nonché da disposizioni impartite da Autorità e da organi di vigilanza e controllo.

- Quali garanzie ho che i miei dati siano trattati nel rispetto dei miei diritti e delle mie libertà personali ?

Il trattamento avverrà nell'ambito degli uffici di segreteria e dei locali scolastici in genere in modalità sia manuale che informatica.
A garanzia della riservatezza dei dati saranno applicate misure minime di sicurezza organizzative ed informatiche di cui viene data evidenza all'interno del "Documento delle misure a tutela dei dati delle
persone" elaborato da questa Istituzione scolastica. L'Istituto ha provveduto ad impartire ai propri incaricati istruzioni precise in merito alle condotte da tenere ad alle procedure da applicare per garantire
la riservatezza dei dati dei propri utenti. In occasione del trattamento potremmo venire a conoscenza di
dati delicati in quanto idonei a rivelare lo stato di salute (certificati medici, infortuni, esoneri, diagnosi
funzionali etc.) e convinzioni religiose (richiesta di fruizione di festività religiose, diete religiose etc.) che, assieme ai dati definiti "giudiziari" vengono trattati per le finalità di rilevante interesse pubblico che il
M.I.U.R. persegue.
Non verrà eseguito su di essi alcun processo decisionale automatizzato (profilazione).

- I miei dati entreranno nella disponibilità di altri soggetti ?

I dati personali forniti potranno essere comunicati agli Enti territoriali, all'Amministrazione scolastica

(M.I.U.R., U.S.R. ed U.S.T.), all'INAIL, all'ASL/ATS oltre che ai professionisti e fornitori di cui il nostro Istituto si avvale quali RSPP, DPO, medico competente, compagnie di assicurazione, agenzie di viaggio, esclusivamente per finalità istituzionali. Specificamente i Suoi dati potrebbero inoltre essere comunicati; ai responsabili del servizio di refezione (se previsto) per i fini organizzativi dello stesso, agli enti esterni per l'organizzazione di attività didattiche di vario genere incluse le uscite didattiche, fotografie che ritraggono gli allievi potranno essere esposte nei locali dell'Istituto ed all'interno delle aule per finalità di
documentazione dell'attività didattica, i dati gestiti in modalità informatica potranno essere visti dai tecnici incaricati della loro custodia in occasione delle attività di controllo e manutenzione della rete e
delle apparecchiature informatiche, i dati degli allievi frequentanti il 3° anno della scuola secondaria di 1°
grado verranno trasmessi alla Regione Lombardia per la costituzione dell'"Anagrafe degli studenti della
regione Lombardia" di cui alla L.R. 19/2007 al fine di attuare il controllo sull'assolvimento degli obblighi di
istruzione e formazione. I dati non saranno comunicati ad altri soggetti non espressamente indicati nella
presente né diffusi se non previo acquisizione del Suo consenso.
In caso di trasferimento il fascicolo personale verrà trasmesso ad altro Istituto destinatario.
I dati non verranno trasferiti a destinatari residenti in paesi terzi rispetto all'Unione Europea né ad organizzazioni internazionali.

- Per quanto tempo terrete i miei dati ?

I dati saranno conservati presso l'Istituto per tutto il tempo in cui l'iscrizione sarà attiva ed in seguito, in
caso di trasferimento ad altra Istituzione o cessazione del rapporto, verranno trattenuti esclusivamente i dati minimi e per il periodo di conservazione obbligatorio previsto dalla normativa vigente.

- Quali sono i miei diritti ?

L'interessato ha diritto di chiedere al Titolare del trattamento:

- L'accesso ai propri dati, la loro rettifica o cancellazione;
- La limitazione e di opporsi al trattamento dei dati personali che lo riguardano;
- La portabilità dei dati;

L'interessato ha inoltre diritto a proporre reclamo all'Autorità di controllo dello Stato di residenza, nonché
a revocare il consenso al trattamento ai sensi dell'Art. 6 del G.D.P.R.

- Cosa accade se non conferisco i miei dati ?

Il mancato, parziale o inesatto conferimento dei dati potrebbe generare quale conseguenza l'impossibilità
di fornire all'allievo tutti i servizi necessari per garantire il suo diritto all'istruzione ed alla

formazione.
Il mancato consenso all'utilizzo delle immagini comporterà l'esclusione dell'allievo dalle attività oggetto di ripresa.

- Chi è il Titolare del trattamento ?

L'Istituto Scolastico nella persona del Dirigente Scolastico pro tempore

Responsabile della
protezione dei dati
(R.P.D. / D.P.O.)

Luca Corbellini
c/o Studio AG.I.COM. S.r.l. - Via XXV Aprile, 12 – 20070 SAN ZENONE AL LAMBRO (MI)
e-mail dpo@agicomstudio.it

Ministero dell'Istruzione, dell'Università e della Ricerca
ISTITUTO COMPRENSIVO DI TURATE
Via Giuseppe Garibaldi, 39 - 22078 Turate (CO)

Tel/fax 02/9688712 - COIC82100L@istruzione.it - COIC82100L@pec.istruzione.it

RICHIESTE DI MANIFESTAZIONE DEL CONSENSO AI SENSI DELL'ART. 7 DEL REGOLAMENTO U.E.

RICHIESTA

ACCONSENTO NON
ACCONSENTO

(APPORRE UNA X NELLE COLONNE A DESTRA IN CORRISPONDENZA DELLA SCELTA FATTA)
Personale autorizzato dall'Istituto potrà fotografare l'allievo in occasione della foto di classe che verrà consegnata anche alle famiglie degli altri allievi coinvolti che ne facciano richiesta.
La comunicazione, oltre che mediante la consegna della fotografia stampata, potrà avvenire anche mediante consegna di file che riproducono le stesse immagini.
Personale autorizzato dell'Istituto potrà riprendere mediante l'ausilio di mezzi audiovisivi, nonché fotografare l'allievo, per fini strettamente connessi all'attività didattica. I risultati di detta attività potranno essere diffusi mediante pubblicazione sul sito internet della scuola o sugli organi di stampa.
I dati dell'allievo, ivi compresi quelli relativi al suo stato di salute, potranno essere comunicati a compagnie assicurative in occasione di infortuni accorsi allo stesso per l'esplicazione delle pratiche di rimborso.
I dati dell'allievo, ivi compresi quelli relativi al suo stato di salute, potranno essere comunicati ai Servizi Sociali del Comune di residenza e/o agli specialisti che hanno in cura il minore al fine di garantire all'alunno il pieno diritto all'istruzione attraverso percorsi personalizzati.
In caso di trasferimento, o al termine del ciclo scolastico, i dati relativi allo stato di salute

dell'allievo potranno essere trasmessi all'Istituto Scolastico di destinazione, in forma riservata, all'interno del fascicolo personale dell'allievo.
I dati anagrafici dell'allievo potranno essere comunicati ad altri Istituti di Istruzione che li richiedano al fine di utilizzarli per informare circa la loro offerta di servizi formativi.

Luogo e data .....
Cognome e nome 1° Genitore ..... Firma ..... (*)
Cognome e nome 2° Genitore ..... Firma .....

(*) Parte da compilare in caso di firma di uno solo degli esercenti la responsabilità genitoriale:
Il sottoscritto, in qualità di genitore/tutore, dichiara avere effettuato la scelta in osservanza delle disposizioni sulla responsabilità genitoriale di cui agli artt. 316, 337 ter e 337 quater del codice civile che richiedono il consenso di entrambi i genitori.
Firma .....

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.

ISTITUTO COMPRENSIVO DI TURATE

REGOLAMENTO D'USO DELLA PIATTAFORMA G SUITE FOR EDUCATION

Il presente Regolamento disciplina l'uso della piattaforma G Suite for Education, attivata dall'Istituto come supporto alla didattica.

Il Regolamento si applica a tutti gli utenti titolari di un account: docenti, studenti e personale ATA e la sua accettazione è condizione necessaria per l'attivazione e l'utilizzo dell'account.

Per gli studenti è indispensabile il consenso firmato da entrambi i genitori.

Copia del Regolamento è pubblicata sul sito dell'Istituto:

1- NATURA E FINALITA' DEL SERVIZIO

a) Il servizio consiste nell'accesso agli applicativi di Google Suite for Education. In particolare ogni utente avrà a disposizione una casella di posta elettronica, oltre alla possibilità di utilizzare tutti i servizi aggiuntivi di G Suite for Education (Drive, Calendar, Moduli, Classroom, ecc) senza la necessità di procedere ad alcuna installazione per la loro funzionalità.

b) Il servizio è inteso come supporto alla didattica e ai servizi correlati con le attività scolastiche in generale: pertanto gli account creati devono essere utilizzati esclusivamente per tali fini.

2- SOGGETTI CHE POSSONO ACCEDERE AL SERVIZIO

a) I docenti (tempo indeterminato e determinato) al momento dell'assunzione fino al termine dell'attività lavorativa presso l'Istituto.

b) Gli studenti, previa compilazione e consegna del modulo di consenso firmato dai

genitori. Il servizio sarà fruibile fino al termine del percorso di studi presso l'Istituto. L'Amministratore ha inoltre limitato la fruibilità del servizio al dominio @icturate.edu.it pertanto essi potranno comunicare via mail e condividere materiali solo con i membri interni all'Organizzazione.

c) Altre categorie di utenti possono richiedere la creazione di un account, per necessità didattiche o di servizio; in questo caso l'accoglimento della domanda è a discrezione del Dirigente Scolastico.

3- CONDIZIONI E NORME DI UTILIZZO

a) Per tutti gli utenti l'attivazione del servizio è subordinata all'accettazione esplicita del seguente Regolamento.

b) L'utente può accedere direttamente dal suo account istituzionale collegandosi al sito dell'Istituto o a Google.it, inserendo il nome utente (attribuito dall'istituzione scolastica) e la password, fornita inizialmente dall'Amministratore o dai suoi delegati e successivamente modificata.

c) Gli account fanno parte del dominio @icturate.edu.it di cui l'Istituto è proprietario.

d) In caso di smarrimento della password l'utente potrà rivolgersi direttamente all'Amministratore o ai suoi delegati.

e) Ogni account è associato ad una persona fisica ed è perciò strettamente personale. Le credenziali di accesso non possono, per nessun motivo, essere comunicate ad altre persone, né cedute a terzi.

f) L'utente accetta pertanto di essere riconosciuto quale autore dei messaggi inviati dal suo account e di essere il ricevente dei messaggi spediti al suo account.

g) Il personale si impegna a consultare giornalmente la propria casella di posta istituzionale a cui saranno inviate circolari e informative.

h) L'utente si impegna a non utilizzare il servizio per effettuare la gestione di comunicazioni e dati personali riservati.

i) L'utente si impegna a non utilizzare il servizio per compiere azioni e/o comunicazioni che arrechino danni o turbative alla rete o a terzi utenti o che violino le leggi ed i Regolamenti d'Istituto vigenti.

j) L'utente si impegna anche a rispettare le regole che disciplinano il comportamento nel rapportarsi con gli altri utenti e a non ledere i diritti e la dignità delle persone.

k) L'utente si impegna a non trasmettere o condividere informazioni che possano presentare forme o contenuti di carattere osceno, blasfemo, diffamatorio o contrario all'ordine pubblico alle leggi vigenti in materia civile, penale ed amministrativa.

l) E' vietato pubblicare in rete materiale che violi diritti d'autore, o altri diritti di proprietà

intellettuale o industriale o che costituisca concorrenza sleale.

m) L'utente s'impegna a non fare pubblicità, a non trasmettere o rendere disponibile attraverso il proprio account qualsiasi tipo di software, prodotto o servizio che violi il presente Regolamento o la legge vigente.

n) L'utente è responsabile delle azioni compiute tramite il suo account e pertanto esonera l'Istituto da ogni pretesa o azione che dovesse essere rivolta all'Istituto medesimo da qualunque soggetto, in conseguenza di un uso improprio.

4- TRATTAMENTO DATI PERSONALI

a) L'Istituto si impegna a tutelare i dati forniti dall'utente in applicazione della normativa vigente in materia di privacy, ai soli fini della creazione e mantenimento dell'account. Il trattamento dei dati è disciplinato da quanto disposto nell'informativa privacy di Google for Education, reperibile all'indirizzo https://gsuite.google.com/terms/education_privacy.html

b) Il servizio è erogato Google che applica la propria politica alla gestione della privacy; l'utente può conoscere in dettaglio tale politica visitando il sito web del fornitore al seguente link: https://www.google.com/intl/it/policies/privacy/

5- NORME FINALI

a. In caso di violazione delle norme stabilite nel presente Regolamento, l'Istituto nella persona del suo rappresentante legale, il Dirigente Scolastico, potrà sospendere l'account dell'utente o revocarlo in modo definitivo senza alcun preavviso e senza alcun addebito a suo carico e fatta salva ogni altra azione di rivalsa nei confronti dei responsabili di dette violazioni.

b. L'Amministratore ha accesso a qualsiasi dato memorizzato negli account creati, inclusa la mail. Pertanto in caso di attività anomale o segnalazioni relative a presunte violazioni del presente Regolamento, l'Amministratore si riserva la possibilità di controllare il contenuto degli account. Per ulteriori informazioni si rinvia al link: https://support.google.com/accounts/answer/181692?hl=it

c. L'Istituto si riserva la facoltà di segnalare alle autorità competenti, per gli opportuni accertamenti ed i provvedimenti del caso, le eventuali violazioni delle condizioni di utilizzo indicate nel presente Regolamento, oltre che delle leggi ed ai regolamenti vigenti.

d. L'account sarà revocato dopo 30 giorni dal termine del percorso di studi presso l'Istituto per gli studenti e del rapporto lavorativo per i docenti ed il personale ATA assunti a tempo indeterminato e determinato (con termine incarico: 30 giugno). Nel caso di supplenze brevi, l'account sarà invece revocato dopo 15 giorni dal termine del contratto. Pertanto i suddetti utenti dovranno provvedere a scaricare e salvare dal proprio account i materiali e i file di interesse entro tale periodo.

MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI "ai sensi della circolare Agid 18 aprile 2017, n. 2/2017

ISTITUTO COMPRENSIVO DI TURATE

ALLEGATO 2 MISURE MINIME DI SICUREZZA INFORMATICA – ISTITUTO COMPRENSIVO DI TURATE

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Realizzare un elenco dei dispositivi utilizzati dall'amministrazione in tutti i suoi plessi collegati alla rete dati.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'aggiornamento avverrà quando saranno aggiunte nuove risorse
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Tali dati sono inseriti nell'archivio delle risorse attive di cui al punto 1.1.1
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	

1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID		Livello		Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	Fare un elenco dei software utilizzati su ogni macchina.
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Periodicamente saranno realizzate dei controlli per verificare che non siano stati installati software non previsti nell'elenco di cui al punto 2.1.1.
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID	Livello	Descrizione	Modalità di implementazione
3 1 1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Per sistemi desktop e server definire dotazione software standard e criteri di gruppo nel domain controller attraverso l'active directory per gestire le richieste di autenticazione per la sicurezza.
3 1 2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
3 1 3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	
3 2 1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Effettuare la configurazione tramite domain controller attraverso l'active directory.
3 2 2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Nel caso in cui un dispositivo risulti compromesso sarà ripristinato alla configurazione standard
3 2 3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3 3 1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini d'installazione di ogni nuovo dispositivo sono memorizzate offline
3 3 2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3 4 1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Tutte le operazioni di amministrazione remota saranno svolte solo attraverso mezzi di connessioni protetti e sicuri

3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Saranno garantite delle scansioni di vulnerabilità dopo ogni aggiornamento significativo dei dispositivo
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	

4	**3**	**1**	**S**	**Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.**	
4	**3**	**2**	**S**	**Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.**	
4	**4**	**1**	**M**	**Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.**	**I software di ricerca delle vulnerabilità sono regolarmente aggiornati**
4	**4**	**2**	**S**	**Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione**	
4	**5**	**1**	**M**	**Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.**	**Le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni sono configurati per avvenire in automatico**
4	**5**	**2**	**M**	**Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.**	**Non vi sono dispositivi air-gapped**
4	**6**	**1**	**S**	**Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.**	
4	**7**	**1**	**M**	**Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.**	**Nel caso fossero saranno riscontrati dei problemi questi saranno risolti attraverso l'installazione di patch o ripristinando il dispositivo.**
4	**7**	**2**	**S**	**Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.**	
4	**8**	**1**	**M**	**Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).**	**Sono state adottate tutte le precauzioni per abbassare al minimo il rischio di sicurezza di ciascun dispositivo utilizzato dall'amministrazione**
4	**8**	**2**	**M**	**Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.**	**Il pericolo è molto basso avendo già previsto che ogni dispositivo si aggiorni automaticamente applicando in tal modo anche le eventuali patch di sicurezza.**

4	**9**	**1**	**S**	**Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.**
4	**10**	**1**	**S**	**Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.**

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID	Livello	Descrizione	Modalità di implementazione

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.

ISTITUTO COMPRENSIVO DI TURATE

REGOLAMENTO LABORATORIO INFORMATICA SCUOLA PRIMARIA

(approvato dal Consiglio di Istituto con delibera n. 39 del 6/11/19)

I laboratori della scuola sono patrimonio comune, pertanto si ricorda che il rispetto e la tutela delle attrezzature sono condizioni indispensabili per il loro utilizzo e per mantenere l'efficienza del laboratorio stesso. Atti di vandalismo o di sabotaggio verranno perseguiti nelle forme previste, compreso il risarcimento degli eventuali danni arrecati. Si invitano gli utenti a rispettare le seguenti indicazioni.

ACCESSO ALL'AULA

Art. 1

l'accesso e l' utilizzo del laboratorio di informatica è consentito per soli scopi didattici:

- **alle classi i inserite nell'orario settimanale di laboratorio (affisso dietro la porta d'ingresso dell'aula), e solo con la presenza del docente della classe;**
- **agli insegnanti con alunni, in coincidenza di spazi orari liberi;**

Art. 2

Il docente che vuole usufruire del laboratorio ritira le chiavi presso la postazione dei collaboratori scolastici e ivi le riconsegna al termine dell'attività. A questo proposito si ricorda che il docente apporrà la firma all'atto del prelevamento e della riconsegna delle chiavi e annoterà eventuali anomalie e danni riscontrati durante lo svolgimento delle attività affinché i docenti responsabili possano esserne informati e dove necessario darne comunicazione al Dirigente Scolastico.

Non è consentita la consegna delle chiavi agli alunni.

Art. 3.

Il laboratorio non deve mai essere lasciato aperto e incustodito quando nessuno lo utilizza.

USO DEI COMPUTER

Art. 4

Ogni insegnante è tenuto a verificare le corrette procedure di accensione/spegnimento da parte degli allievi e a verificare l'integrità dei PC. Qualora si riscontrssero mal funzionamenti o mancanze, l'insegnante di classe dovrà riferirlo prontamente, senza manipolare alcunché, ai Responsabili di laboratorio e annotarlo sul REGISTRO.

Art. 5

Ogni insegnante può far salvare i file realizzati durante la sessione di lavoro nella cartella della propria fascia di classe, creata dentro la cartella "CONDIVISA" presente in "COMPUTER". Al termine dell'anno scolastico queste cartelle saranno svuotate.

Art. 6

Ogni docente deve prestare attenzione affinché gli alunni non cancellino erroneamente i file delle altre classi.

Art. 7

È vietata assolutamente qualsiasi manomissione o cambiamento dell'hardware o del software delle macchine.

Art. 8

È assolutamente vietato agli alunni variare le impostazioni del computer (desktop, screensaver, etc...), come pure installare o disinstallare programmi di qualunque natura, trasferire dati da supporti removibili, creare cartelle, copiare, spostare, rinominare o cancellare files senza esplicite indicazioni da parte del docente. Non è permesso, altresì, utilizzare i computer per giocare o per svolgere attività personali.

Art.9

Gli insegnanti possono chiedere di installare nuovi software sui PC del laboratorio, previa autorizzazione del Dirigente, ai Responsabili del laboratorio.

Art.10

Le attrezzature hardware e gli altri materiali in dotazione al laboratorio non possono essere destinati, neanche temporaneamente, ad altre attività esterne all'aula medesima ad eccezione dei Tablet, custoditi nell'apposito carrello corredato di caricatori.

Art.11

La postazione server è destinata all'insegnante; nessun altro potrà utilizzare tale postazione (se non in presenza o con l'autorizzazione dell' insegnante).

USO DI INTERNET

Art.12

È assolutamente vietato l'uso di Internet agli alunni e non per ricerche o lavori programmati dall'insegnante e in sua vigile e costante presenza. È compito degli insegnanti accompagnatori controllare i materiali scaricati dagli alunni durante la navigazione.

2

Art.13

L 'accesso a Internet, anche da parte degli adulti, può avvenire solo per motivi connessi all'attività didattica. L'uso che viene fatto di Internet deve essere esclusivamente di comprovata valenza didattica.

Art.14

È vietato alterare le opzioni del software di navigazione.

USO DELLA STAMPANTE

Art.15

L'uso della eventuale stampante presente in laboratorio è riservato solamente agli insegnanti, seguendo le apposite istruzioni fornite dai Responsabili. Per quanto riguarda le cartucce e il toner, occorre fare attenzione ed evitare gli sprechi.

NORME GENERALI DI COMPORTAMENTO

Art.16

È assolutamente vietato portare cibi e bevande nel laboratorio, né tantomeno appoggiare bottigliette d'acqua o bicchieri i tavoli.

Art.17

Prima di uscire dal laboratorio occorre accertarsi che tastiera, mouse, sedia e quant'altro siano al loro posto, che non vi siano cartacce o rifiuti e che TUTTE LE APPARECCHIATURE ELETTRICHE SIANO SPENTE.

COMPITI DEI RESPONSABILI DI LABORATORIO

Art.18

I Responsabili di laboratorio, non essendo dei tecnici, hanno la funzione di supervisione, coordinamento e verifica della corretta applicazione di quanto indicato nel presente regolamento, riferendo eventuali anomalie riscontrate al Dirigente Scolastico.

ISTITUTO COMPRENSIVO DI TURATE

REGOLAMENTO LABORATORIO DI INFORMATICA

SCUOLA SECONDARIA DI I GRADO

I laboratori della scuola sono patrimonio comune, pertanto si ricorda che il rispetto e la tutela delle attrezzature sono condizioni indispensabili per il loro utilizzo e per mantenere l'efficienza del laboratorio stesso. Atti di vandalismo o di sabotaggio verranno perseguiti nelle forme previste, compreso il risarcimento degli eventuali danni arrecati. Si invitano gli utenti a rispettare le seguenti indicazioni:

Norme di accesso

Art.1- l'accesso al laboratorio di informatica è subordinato all'accettazione del presente regolamento;

Art.2- l'accesso è riservato ai docenti e agli studenti del nostro istituto, e previa autorizzazione del dirigente scolastico, agli utenti esterni nell'ambito di progetti extracurricolari in orario pomeridiano;

Art.3- l'accesso all'aula avviene previa prenotazione su apposito modulo affisso sulla porta del laboratorio;

Art.4- il docente che vuole usufruire del laboratorio ritira le chiavi presso la postazione dei collaboratori scolastici e ivi le consegna al termine dell' attività;

Art.5- ogni studente potrà utilizzare il laboratorio esclusivamente per svolgere lavori inerenti a progetti scolastici o ad attività didattica, in ogni caso mai da solo ma con un insegnante referente di riferimento;

Art.6- gli utenti che a qualunque titolo utilizzano l'aula dovranno compilare il relativo registro inserendo i seguenti dati: classe, docente, ora di inizio e fine di attività, e se utente singolo: nome, cognome, numero postazione usata, ora di inizio e fine di attività, è auspicabile che i docenti assegnino ad ogni allievo, o gruppo la propria postazione tramite apposito modulo;

Norme di utilizzo del materiale informatico

Art.7- l'utilizzo delle attrezzature informatiche è consentito esclusivamente per scopi inerenti la didattica;

Art.8- il docente durante l'ora a sua disposizione per lezioni o esercitazioni osserverà la massima vigilanza sul comportamento degli alunni e sul rispetto degli stessi per il materiale informatico e per le attrezzature in dotazione dell'aula; inoltre, segnalerà al responsabile qualsiasi guasto o malfunzionamento riscontrato;

Art.9- è assolutamente vietato spostare, copiare, o cancellare files appartenenti al sistema operativo o ai programmi installati ed inoltre installare, modificare o rimuovere applicazioni dai computer dell'aula, modificare la configurazione di sistema e in generale porre in essere ogni comportamento che possa danneggiare l'hardware o il software installato;

Art.10- è vietato installare e utilizzare programmi personali sul computer;

Art.11- è vietato scaricare programmi da internet per utilizzarli sui computer dell'aula;

Art.12- è vietata la navigazione su siti internet potenzialmente pericolosi e/o illegali. L'uso di Internet va fatto sotto stretto controllo dei docenti;

Art.13- si consiglia di memorizzare i propri dati solo su pen drive personali. È possibile memorizzare dati solo temporaneamente su apposite cartelle comuni, che verranno però periodicamente ripulite;

Art.14- il personale e gli alunni dovranno avere cura di rispettare le procedure corrette di accensione, di utilizzo e di spegnimento delle macchine;

Art.15- è vietato spostare i computer portatili dalla postazione prefissata;

Norme generali di comportamento

Art.16- nell'aula è vietato mangiare, bere e disturbare in altri modi lo svolgimento delle attività di studio;

Art 17- quando si lascia il laboratorio accertarsi che

- **la postazione di lavoro sia pulita e in ordine;**
- **i computer e le stampanti siano spenti;**
- **la porta sia stata chiusa a chiave.**

ISTITUTO COMPRENSIVO DI TURATE

REGOLAMENTO USO LIM

Premessa

La Lavagna Interattiva Multimediale (LIM) è un BENE COMUNE DI TUTTI. Docenti e alunni sono responsabili del buon utilizzo di questo costoso strumento da utilizzare con cura e accortezza.

Compiti dei Docenti

• Il docente della prima ora antimeridiana e pomeridiana deve ritirare la chiave di accesso al box contenente il PC portatile presso l'armadio individuato dal team;

• Il docente dell'ultima ora antimeridiana e pomeridiana deve spegnere tutta l'apparecchiatura e riporre le chiavi dove concordato;

• Sincerarsi delle condizioni delle attrezzature connesse alla LIM all'inizio e alla fine del suo utilizzo;

• Segnalare ai responsabili del supporto tecnologico/LIM eventuali problemi tecnici e/o di altra natura riscontrati;

• Non lasciare che gli alunni utilizzino la LIM in autonomia,ma supervisionare sempre che essa venga usata nel modo corretto;

• Dopo aver utilizzato la penna riporla nella apposita scatola fissata al muro; • Aver cura che la penna non venga danneggiata;

• OCCUPARSI DI RICARICARE LE BATTERIE necessarie al corretto funzionamento della penna con il caricabattiere in dotazione;

• Nel ricaricare le batterie assicurarsi che siano adatte a tale funzione;

• Utilizzare le BATTERIE NON RICARICABILI esclusivamente per il TELECOMANDO (quando necessarie richiederle ai responsabili);

• Alla fine della sessione di lavoro verificare (quando possibile) se la LIM sarà utilizzata dal collega dell'ora successiva:in caso positivo è consentito lasciare PC e proiettore accesi, in caso contrario sarà opportuno spegnerli.

1

• Compiti degli alunni

Ogni alunno:

• è tenuto a chiedere sempre il permesso all'insegnante prima di poter accendere ed utilizzare la LIM;

• durante le sessioni di lavoro è responsabile dell'attrezzatura che gli è messa a disposizione e risponde di eventuali danni arrecati:per questo deve usare la LIM unicamente sotto la supervisione di un insegnante.

• DIVIETI

È assolutamente vietato:

• Modificare la configurazione originaria della LIM e dei suoi componenti; ogni variazione del sistema va segnalata ai docenti responsabili;

• Installare, rimuovere, copiare programmi senza l'autorizzazione del docente responsabile.

• INTERVENTO DEI DOCENTI RESPONSABILI

I responsabili per le LIM, ricevute le segnalazioni di eventuali problemi tecnici e/o di altra natura, interverranno compatibilmente con il proprio orario di servizio.

P.S.

• Prima di chiedere l'intervento dei responsabili assicurarsi che tutti i collegamenti siano stati effettuati correttamente.

• Per la penna interattiva assicurarsi che sia dotata di batteria carica.

2

• ISTRUZIONI PER L'UTILIZZO DELLA LIM

Per ACCENDERE correttamente la LIM:

• ritirare la chiave di accesso al box;

• aprire il tool-box;

• ABBASSARE LA RIBALTINA CON MOLTA CAUTELA CONTROLLANDO CHE I COLLEGAMENTI NON RESTINO AGGROVIGLIATI;

• accendere la ciabatta (ove presente);

• accendere il PC;

• accendere il proiettore.

Per SPEGNERE correttamente la LIM:

• spegnere il proiettore cliccando due volte il tasto accensione/spegnimento del telecomando;

• spegnere il PC, come di consueto;

• spegnere la ciabatta(ove presente);

• ALZARE LA RIBALTINA CON MOLTA CAUTELA CONTROLLANDO CHE I COLLEGAMENTI NON RESTINO AGGROVIGLIATI;

• chiudere il tool-box;

• depositare le chiavi nell'armadio individuato dal team.

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.

ISTITUTO COMPRENSIVO DI TURATE

Regolamento per l'uso dei telefoni cellulari e dispositivi mobili a scuola

APPROVATO DAL CONSIGLIO DI ISTITUTO in data 19 settembre 2016.

Sezione A: uso da parte del personale.

Art. 1 - disposizioni

Il personale in servizio può utilizzare il telefono cellulare o altri dispositivi mobili esclusivamente nei seguenti casi:

1. **Se preventivamente autorizzato dal DS (personale docente) o dal DSGA (personale ATA).**
2. **Se l'utilizzo è connesso allo svolgimento della propria funzione, es. uso del registro elettronico o attività legate alla sicurezza sui luoghi di lavoro.**
3. **In caso di grave e comprovata urgenza, da documentare.**

L'utilizzo in altri casi è espressamente vietato e soggetto a sanzione disciplinare.

Nei casi di utilizzo in presenza degli alunni, per coerenza del messaggio educativo, è opportuno comunicare agli stessi la motivazione d'uso.

Si rammenta che è parimenti vietato l'utilizzo delle risorse della scuola (postazioni computer, stampanti, fotocopiatrici ecc.) per attività non inerenti la prestazione lavorativa. Durante la navigazione in internet e, in generale, in ogni utilizzo delle risorse scolastiche, è di particolare importanza astenersi da qualsiasi attività che possa compromettere la sicurezza informatica della rete di Istituto.

Sezione B: uso da parte degli alunni.

Art. 2 – uso del telefono cellulare per chiamate, sms, messaggistica in genere

Si ribadisce la puntuale applicazione della normativa vigente (DPR 249/1998, DPR 235/2007, Direttiva Ministeriale 15.03.2007), pertanto l'uso del cellulare in quanto tale non è consentito per ricevere/effettuare chiamate, SMS o altro tipo di messaggistica (es. Whatsapp). La comunicazione con le famiglie, per qualsiasi urgenza, è sempre garantita attraverso il telefono della scuola.

Il divieto non si applica soltanto all'orario delle lezioni ma è vigente anche negli intervalli e nelle altre pause dell'attività didattica. L'estensione del divieto d'uso ai momenti di pausa risponde ad un'esigenza prettamente educativa, tesa a favorire la socializzazione e le relazioni dirette tra le persone, dal momento che è piuttosto evidente la tendenza dei ragazzi ad "isolarsi" attraverso l'operatività sui propri dispositivi mobili.

Gli alunni sono tenuti a mantenere i loro telefoni spenti durante l'intera permanenza a scuola, salvo nei casi di utilizzo autorizzato. In ogni caso si deve evitare di essere raggiunti da qualsiasi notifica o segnalazione, eventi particolarmente distraenti e disturbanti durante l'attività didattica.

I docenti possono consentire l'uso del cellulare, in caso di particolari situazioni non risolvibili in altro modo. L'autorizzazione deve essere preventivamente richiesta e supportata da idonea motivazione, da annotare sul registro di classe.

Le famiglie sono invitate a collaborare strettamente con l'Istituto, nello spirito della corresponsabilità educativa, evitando ad esempio di inviare messaggi o effettuare chiamate ai telefoni dei propri figli durante l'orario scolastico.

In particolare per la scuola primaria si suggerisce ai genitori di non consentire ai bambini di portare a scuola il telefono cellulare, per limitare i rischi di danneggiamento, furto, uso improprio.

Art. 3 – uso di telefoni o dispositivi per altre funzioni (foto, video, applicazioni varie)

a) Utilizzo nell'ambito dell'attività didattica

L'utilizzo dei dispositivi mobili può essere autorizzato dal docente per lo svolgimento di attività didattiche innovative e collaborative, che prevedano anche l'uso di dispositivi tecnologici e l'acquisizione da parte degli alunni di un elevato livello di competenza

digitale, soprattutto per quanto riguarda l'uso consapevole e responsabile delle tecnologie. Si ricorda che la competenza digitale è una delle competenze chiave per l'apprendimento permanente, identificate dall'Unione Europea.
L'uso di smartphone, tablet e altri dispositivi mobili, o delle funzioni equivalenti presenti sui telefoni cellulari è pertanto consentito, ma unicamente su indicazione del docente, con esclusiva finalità didattica, in momenti ben definiti e con modalità prescritte dall'insegnante.

b) Registrazione delle lezioni

Secondo le recenti indicazioni del Garante della privacy, la registrazione delle lezioni è possibile per usi strettamente personali. Qualora gli alunni intendessero avvalersi di tale possibilità, sono tenuti a informare l'insegnante prima di effettuare registrazioni audio/foto/video delle lezioni o di altre attività didattiche. In nessun caso le riprese potranno essere eseguite di nascosto, senza il consenso dell'insegnante.

c) Diffusione

Si ribadisce che registrazioni e riprese audio/foto/video sono consentite per uso personale, mentre la diffusione di tali contenuti è invece sempre subordinata al consenso da parte delle persone registrate/ritratte/riprese.

Si richiama l'attenzione degli alunni, dei docenti e delle famiglie sulle possibili conseguenze di eventuali riprese audio/video o fotografie effettuate all'interno degli ambienti scolastici, al di fuori dei casi consentiti, e successivamente diffuse con l'intento di ridicolizzare compagni o insegnanti o addirittura allo scopo di intraprendere azioni che sono spesso definite con il termine di cyberbullismo. Tali azioni possono configurare, nei casi più gravi, gli estremi di veri e propri reati.

Anche in questo caso si ravvisa la necessità di grande sintonia e collaborazione tra scuola e famiglia, nell'ottica di favorire negli alunni lo sviluppo della necessaria consapevolezza e maturità nell'uso dei potenti strumenti ai quali hanno accesso. La scuola promuove iniziative di informazione e formazione sui temi dell'uso consapevole dei dispositivi informatici, dei nuovi media, dei social network e in generale delle applicazioni web e mobili. Tali iniziative sono rivolte principalmente agli alunni ma anche, ove possibile, alle famiglie.

Art. 4 – disposizioni in caso di uscita didattica

Per quanto riguarda uscite, visite guidate e viaggi di istruzione, è consentito l'uso dei dispositivi mobili per garantire le comunicazioni con il gruppo e per documentare le attività.

I docenti potranno autorizzare l'uso moderato per intrattenimento purché al di fuori dei momenti dedicati a visite guidate e attività legate all'aspetto didattico dell'uscita.

I dispositivi dovranno comunque essere utilizzati nel pieno rispetto delle esigenze altrui.

Si rammenta quanto già esposto in merito alla eventuale diffusione delle immagini.

Art. 5 - sanzioni

In generale, ogni utilizzo non autorizzato dei telefoni o dispositivi, al di fuori di quanto previsto in precedenza, non è permesso e sarà sanzionato.

In caso di prima contravvenzione al presente regolamento si provvederà ad informare la famiglia tramite annotazione sul diario personale e sul registro.

In caso di contravvenzione ripetuta si provvederà ad informare telefonicamente la famiglia; il dispositivo sarà ritirato e restituito solo al termine delle lezioni al genitore o all'adulto da questi delegato al ritiro dell'alunno.

Come per ogni altra infrazione al regolamento di Istituto, l'utilizzo non autorizzato dei telefoni o dispositivi sarà considerato nell'attribuzione del giudizio sul comportamento dell'alunno in sede di valutazione intermedia e/o finale, con conseguenze proporzionali alla gravità dell'infrazione stessa. Si rimanda ai criteri per la valutazione del comportamento inseriti nel PTOF.

Il nostro piano d'azioni

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

- 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

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

- 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)
- 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)

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.*

I rischi legati all'uso non consapevole della rete da parte dei minori sono molto alti ed aprono il delicato capitolo del rispetto della sicurezza nell'uso delle Tic (cyberbullismo, violazione della privacy, adescamento online, sexting, pedopornografia, gioco d'azzardo...).

Tali pericoli rendono necessaria, da parte della scuola, un'azione di sensibilizzazione generale affinchè:

- venga raggiunta piena consapevolezza dell'esistenza del problema sia tra i docenti, sia tra gli alunni;

- giovani e adulti sappiano che è prioritario tutelare la privacy propria e dei compagni di lavoro;

- si effettui un'azione di prevenzione delle infrazioni grazie al rinforzo di comportamenti positivi e collaborativi;

- si giunga alla sensibilizzazione di tutta la comunità scolastica.

La scuola si avvale della collaborazione delle forze dell'ordine del territorio per organizzare incontri di sensibilizzazione e informazione rivolti agli alunni della scuola secondaria di primo grado e ai loro genitori.

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).

Spesso la convinzione di essere tutelati dall'anonimato toglie agli aggressori i freni inibitori e li spinge ad essere sempre più crudeli.

Per prevenire il cyberbullismo, le istituzioni scolastiche devono pianificare un intervento che investa su più sfaccettature del problema:

- la prevenzione grazie alla sensibilizzazione degli studenti;

- lo sviluppo di peer education tra alunni;

- la formazione del corpo docenti;

- lo sviluppo delle competenze digitali degli alunni sin dalla più giovane età;

- l'elaborazione di misure di sostegno e rieducazione dei minori coinvolti;

-l'integrazione dei principali riferimenti al cyberbullismo nel patto di corresponsabilità con i genitori.

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.

Per contrastare l'istigazione all'odio è necessario responsabilizzare gli studenti affinchè sappiano opporsi a tali condotte lesive.

Gli insegnanti possono stimolare la partecipazione delle classi ad attività sociali, attivarsi per distruggere concetti discriminatori come la differenza di razza, religione e genere tra i loro studenti. E' importante segnalare i casi di hate speech o di cyberbullismo affinchè gli alunni siano in grado di:

- evitare di condividere, commentare o mettere like a post offensivi;

- se l'hater è un amico o conoscente, cercare di sensibilizzarlo a un comportamento positivo in rete;

- segnalare pagine o gruppi intolleranti o offensivi;

- non rispondere ai commenti di chi provoca per scatenare litigi o malumore (troll) e segnalarli.

4.4 - Dipendenza da Internet e gioco online

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

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

La scuola ha il dovere di favorire il "benessere digitale" tra i suoi alunni e, per tale scopo, può stimolare questi ultimi affinchè:

- utilizzino internet in modo equilibrato;

- considerino la tecnologia come mezzo per il raggiungimento di obiettivi ben definiti e non come fine utile a se stesso;

- interagiscano on-line con responsabilità e gestiscano con sicurezza il "sovraccarico informativo".

Inoltre è fondamentale responsabilizzare le famiglie affinché vigilino su tempi e modi di utilizzo delle tecnologie nel tempo libero.

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.

Per prevenire o intervenire in caso di tali problematiche, la scuola si attiverà per:

- organizzare attività di informazione per studenti e docenti;

- rassicurare gli alunni e renderli consapevoli dell'importanza di comunicare il proprio disagio all'adulto di riferimento;

- analizzare le situazioni problematiche in un'ottica di dialogo formativo e fiducia;

- investire sul valore di ciascuno;

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.

In caso di grooming, il personale docente ha il dovere di denunciare gli episodi lesivi alla polizia postale e di fornire un supporto psicologico alla vittima dell'adescamento on line attivando le agenzie sanitarie del territorio come ilconsultorio o neuropsichiatria.

In tali frangenti potrà essere utile contattare l'helpline di Generazioni connesse e il numero dedicato di telefono azzurro.

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.

In caso di pedopornografia il personale docente ha il dovere di denunciare gli episodi lesivi alla polizia postale e di fornire un supporto psicologico alla vittima dell'adescamento on line attivando le agenzie sanitarie del territorio come il consultorio o neuropsichiatria.

In tali frangenti potrà essere utile contattare l'helpline di Generazioni connesse e il numero dedicato di telefono azzurro.

Il nostro piano d'azioni

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

☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

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

☐ 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 ai genitori e ai docenti, con il coinvolgimento di esperti.

☐ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

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.

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.

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.

PROGETTO LA RETE Si-Cura

LINEE GUIDA SPERIMENTALI PER L'EFFICACE GESTIONE IN RETE DI SITUAZIONI DI MALTRATTAMENTO E VIOLENZA ASSISTITA FAMILIARE A DANNO DI MINORENNI DI CUI EMERGE NOTIZIA NEGLI ISTITUTI COMPRENSIVI DELL'AMBITO TERRITORIALE SOCIALE DI LOMAZZO – FINO MORNASCO

INDICE

1

LA CORNICE PROGETTUALE

Il progetto "LA RETE Si-Cura" nasce dall'esigenza di rinforzare l'azione preventiva relativamente ai fenomeni del maltrattamento agito contro i minori e della violenza assistita intrafamiliare anche a fronte di un crescente numero di situazioni complesse di questo tipo riscontrate all'interno dell'ambito territoriale di riferimento.

Dall'analisi dei bisogni - rilevati principalmente attraverso il Servizio di Psicologia Scolastica - si è evinta la necessità definire e successivamente implementare linee guida per una corretta gestione in rete della casistica, elaborandole e condividendole con i principali soggetti della rete medesima, ovvero gli Istituti Scolastici pubblici, i Servizi Sociali comunali, l'équipe del Servizio di Psicologia Scolastica di ASCI.

Finalità principale della progettazione è la costituzione di una rete di interlocutori chiara e stabile che si configuri come un "luogo sicuro", ovvero che garantisca la tutela di tutti i soggetti coinvolti, in primis dei minorenni, e l'efficacia dei percorsi attivati.

La progettualità è stata preceduta da una prima fase di mappatura, avvenuta mediante la somministrazione di un questionario, per rilevare il punto di vista dei docenti dei 9 ICS del Distretto relativamente alle tematiche in oggetto. Ne è conseguito un percorso formativo rivolto agli insegnanti di scuola dell'infanzia, primaria e secondaria di primo grado; agli Assistenti Sociali operanti nel Distretto e agli psicologi del Servizio di Psicologia Scolastica dell'ASCI, che ha coinvolto circa 300 partecipanti.

Successivamente alla formazione, sono stati sviluppati tavoli tecnici d i confronto e condivisione con i differenti soggetti della rete coinvolti e con l'Arma dei Carabinieri e la Polizia di Stato, al fine di prefigurare i contenuti e le indicazioni metodologiche principali necessarie per strutturare la procedura.

La progettazione è stata inoltre condivisa all'interno del Tavolo Tematico Minori e Famiglie nell'ambito della progettazione del Piano di Zona per il triennio 2017 - 20 e successivamente inserita negli obiettivi del Piano di Zona medesimo.

2

PROCEDURA IN SITUAZIONI DI PREGIUDIZIO CON ELEMENTI DI REATO IPOTIZZATI PERSEGUIBILI D'UFFICIO

I PRESUPPOSTI

Il lavoro di confronto con i differenti soggetti della rete ha concordato che oggetto della presente procedura sperimentale siano le situazioni di pregiudizio, sospetto o conclamato, che possano configurare anche elementi di reato perseguibile d'ufficio (vedi allegato n.1).

Centralità nell'articolazione della procedura è la cura del lavoro di rete e della comunicazione tra gli interlocutori della rete. In tale direzione, la risorsa fondamentale è rappresentata dallo strumento dell'Équipe Multidisciplinare, così composta:

▯ il dirigente scolastico dell'Istituto Comprensivo in cui viene rilevata la situazione

▯ l'insegnante o gli insegnanti coinvolti nella rilevazione dei fatti

▯ l'assistente sociale del servizio di base del comune di residenza del minorenne o dei minorenni coinvolti

▯ lo psicologo scolastico del Servizio di Psicologia Scolastica ASCI dell'Istituto Comprensivo in cui si rileva la situazione

IL PERCORSO

Rilevazione

La situazione di maltrattamento e/o di violenza assistita intrafamiliare può essere rilevata a scuola sia dall'insegnante che dallo psicologo scolastico.

Il soggetto che rileva all'interno del contesto scolastico una situazione che si configura come reato, sospetto o conclamato, perseguibile d'ufficio, informa il dirigente scolastico, sia a voce che mediante relazione scritta (vedi allegato n.2).

Attivazione dell'Équipe Multidisciplinare

In situazioni in cui non si deve intervenire con l'urgenza non avendo evidenza dell'effettiva esistenza del reato e del rischio per il minore nel permanere presso i propri familiari, il dirigente scolastico convoca l'incontro in Équipe Multidisciplinare in tempi ristretti, non superiori ai cinque giorni lavora tivi.

La convocazione verrà inoltrata dal dirigente scolastico per posta elettronica ai servizi sociali e al servizio di psicologia scolastica senza inserire dati particolari o, in alternativa, in forma criptata.

3

Se il minorenne è di origine straniera, qualora si evidenzi la necessità di una consulenza transculturale, il Dirigente Scolastico ha il compito di coinvolgere nell'Équipe Multidisciplinare l'operatore del progetto ASCI Link, seguendo le procedure già attive e

concordate con gli ICS.

L'assistente sociale del Servizio Sociale di base ha il compito di coinvolgere nell'incontro di Équipe Multidisciplinare:

- l'operatore del Servizio Tutela Minori, qualora il minorenne sia già in carico presso il Servizio Tutela minori competente per territorio;

- l'educatore scolastico e/o di assistenza educativa domiciliare, se assegnato al minorenne e se la sua partecipazione sia ritenuta pertinente, mediante contatto con il Coordinatore dei Servizi Educativi Minori ASCI.

Obiettivi dell'Équipe Multidisciplinare sono:

favorire la condivisione degli elementi informativi tra i soggetti della rete coinvolti

facilitare l'emersione e il confronto tra i possibili e differenti punti di vista in merito alla situazione

riconoscere e condividere ruoli e responsabilità di ciascun soggetto della rete

definire la fase operativa successiva (Es.: segnalazione; monitoraggio; etc.) e la relativa tempistica

definire l'incontro successivo in Équipe Multidisciplinare.

I contenuti dell'incontro verranno formalizzati in un verbale a cura del dirigente scolastico e sottoscritti da ciascuno dei presenti (vedi allegato n.3). Copia del verbale firmato potrà essere consegnata in forma cartacea ai presenti oppure inviato per posta elettronica in modalità criptata.

Segnalazione all'Autorità Giudiziaria

Sarà compito del Dirigente Scolastico inoltrare la relazione di segnalazione alla Procura della Repubblica presso il Tribunale per i Minorenni e/o, a seconda della tipologia di situazione, alla Procura della Repubblica presso il Tribunale Ordinario.

La segnalazione verrà inoltre inviata per conoscenza ai Servizi Sociali del Comune di residenza del/i minorenne/i coinvolto/i nella situazione e alla Stazione dei Carabinieri competente per territorio.

4

Monitoraggio

Si prevede un'azione di monitoraggio della situazione da parte dell'Équipe Multidisciplinare attraverso la valorizzazione del ruolo e delle competenze di ciascuno dei suoi componenti.

Nella fattispecie:

▯ il servizio sociale manterrà la regia dell'intervento

▯ il dirigente scolastico e il corpo docente coinvolto provvederanno a mettere in campo azioni atte a favorire il benessere a scuola dei minorenni coinvolti

▯ lo psicologo scolastico, attraverso gli strumenti dell'osservazione in classe e della consulenza diretta agli insegnanti e al dirigente scolastico, contribuirà a facilitare la cura della comunicazione a scuola relativamente alla situazione in oggetto e a favorire il benessere a scuola dei minorenni coinvolti (singoli soggetti e/o gruppo classe) e del corpo docente.

Le azioni di monitoraggio verranno concordate e condivise all'interno degli incontri dell'Équipe Multidisciplinare.

5

SINTESI GRAFICA DELLA PROCEDURA

Comunicazione scritta al Dirigente Scolastico di

quanto rilevato/osservato a scuola;

Dirigente Scolastico convoca l'Equipe

Multidisciplinare entro 5 gg. lavorativi

Equipe Multidisciplinare (dirigente scol.; assistente

servizi sociali comunali; psicologo scol. ASCI)

SEGNALAZIONE

SI'

Il Dirigente invia la segnalazione, alla Procura Competente e p.c. ai Servizi Sociali Comunali e ai Carabinieri competenti per Territorio;

SEGNALAZIONE

NO

L'Equipe Multidisciplinare definisce un tempo di osservazione/ monitoraggio e concorda un'ulteriore data in cui riunirsi per rivalutare il caso.

6

CLASSIFICAZIONE DELLE FORME DI MALTRATTAMENTO E ABUSO

Riportiamo di seguito una sintetica classificazione delle forme di maltrattamento e abuso

all'infanzia, utile a fini esemplificativi. È tuttavia opportuno sottolineare come più frequentemente il minorenne sia vittima di "costellazioni" di maltrattamenti che possono assumere forme diverse.

Maltrattamento fisico

Si intende il ricorso sistematico alla violenza fisica come aggressioni, punizioni corporali o gravi attentati all'integrità fisica, alla vita del bambino/adolescente e alla sua dignità. "Questo include il colpire, percuotere, prendere a calci, scuotere, mordere, strangolare, scottare, bruciare, avvelenare, soffocare. Gran parte della violenza a danno di minori dentro le mura domestiche viene inflitta con lo scopo di punire" (WHO, 2006). Si intende anche il fallimento nel prevenire un danno fisico dovuto ad aggressioni, punizioni corporali, gravi attentati all'integrità fisica del minorenne. Possono essere inquadrate come maltrattamento fisico anche le mutilazioni genitali femminili.

Maltrattamento psicologico

Si intendono comportamenti e frasi che si configurano come pressioni psicologiche, ricatti affettivi, minacce, intimidazioni, discriminazioni, indifferenza e rifiuto volti a provocare umiliazione, denigrazione e svalutazione in modo continuato e duraturo nel tempo. Rientra in tale categoria anche il coinvolgimento del figlio minorenne nelle separazioni coniugali altamente conflittuali, ch e comportano il suo attivo coinvolgimento in strategie volte a denigrare, svalutare, alienare, rifiutare un genitore.

Violenza assistita

Si intende l'esperire da parte del bambino/a qualsiasi forma di maltrattamento compiuto attraverso atti di violenza fisica, verbale, psicologica, sessuale ed economica su figure di riferimento o su altre figure affettivamente significative adulte o minori. Il bambino può farne esperienza direttamente (quando essa avviene nel suo campo percettivo), indirettamente (quando il minore è a conoscenza della violenza), e/o percependone gli effetti. Si include l'assistere a violenze di minori su altri minori e/o su altri membri della famiglia e ad abbandoni e maltrattamenti ai danni di animali domestici (CISMAI, 2006). È considerata un maltrattamento primario, al pari del maltrattamento fisico, psicologico, dell'abuso sessuale, della trascuratezza. Rappresenta un fattore di rischio altamente predittivo per le altre forme di maltrattamento.

7

Patologia delle cure

Si configura allorché i genitori o le persone legalmente responsabili del minorenne non provvedono adeguatamente ai suoi bisogni fisici, psichici e affettivi, in rapporto alla fase evolutiva. Comprende:

Incuria/trascuratezza grave. S'intende qualsiasi atto omissivo prodotto da una grave incapacità del genitore nel provvedere ai bisogni del figlio, che comporta un rischio imminente e grave per il bambino quale abbandono, rifiuto, grave compromissione dello

sviluppo fisico, cognitivo, emotivo o altre forme di abuso e violenza, fino al decesso. E' spesso non rilevata e scarsamente riconosciuta, frequentemente associata ad altre forme di maltrattamento. E' ormai condiviso e riconosciuto dalla letteratura scientifica che la trascuratezza grave può essere non meno dannosa di altre forme di maltrattamento.

Discuria Si realizza quando le cure vengono fornite in modo distorto, non appropriato o congruo alla fase evolutiva del bambino, comportando l'imposizione di ritmi di acquisizione precoci, aspettative irrazionali, eccessiva iperprotettività.

Ipercura Si realizza quando le cure fisiche sono caratterizzate da una persistente ed eccessiva medicalizzazione da parte di un genitore, generalmente la madre e si distinguono le seguenti forme: 1. il "Medical Shopping per procura" è una condizione nella quale uno o entrambi i genitori, molto preoccupati per lo stato di salute del bambino a causa di segni/ sintomi modesti, lo sottopongono a inutili ed eccessivi consulti medici, 2. nel "Chemical Abuse" vengono somministrate al bambino dai genitori, di propria iniziativa, sostanze o farmaci che possono essere dannose allo scopo di provocare sintomi che richiamino l'attenzione dei sanitari; 3. nella "Sindrome di Münchausen per procura (MPS)" un genitore, generalmente la madre, attribuisce al figlio malattie inesistenti, frutto di una convinzione distorta circa la propria salute, poi trasferita sul bambino che tende successivamente a colludere con questo atteggiamento simulando i sintomi di malattie.

Abuso sessuale

Si intende il coinvolgimento del minore in attività sessuali, anche se percepite piacevoli, da parte di un partner preminente; si intendono abusi sessuali anche modalità seduttive non caratterizzate da violenze esplicite, se perpetrate da un adulto. Le manifestazioni dell'abuso sessuale possono concretizzarsi con atti di libidine occasionali (carezze, esibizionismo), atti di libidine reiterati, violenza sessuale assistita, induzione alla visione di materiale pornografico, rapporti sessuali, avvio alla prostituzione, utilizzo del minore per la produzione di materiale pornografico, incesto, pedofilia. A seconda del rapporto esistente tra il bambino e l'abusante, l'abuso sessuale può suddividersi in: - intra-familiare, attuato da membri della famiglia nucleare o allargata - peri-familiare, attuato da persone conosciute dal minore, comprese quelle a cui è affidato per ragioni di cura/educazione. Queste due forme di abuso sono le più frequenti. - extra familiare, se l'abusante è una figura estranea all'ambiente familiare e al minore. L'abuso sessuale è raramente un atto violento che lascia segni fisici. A fronte della frequente aspecificità sintomatologica sono particolarmente orientativi i comportamenti sessualizzati inadeguati per l'età dello sviluppo, soprattutto se caratterizzati da compulsività e pervasività.

8

Sfruttamento sessuale

E' il comportamento di chi percepisce danaro od altre utilità, da parte di singoli o di gruppi criminali organizzati, finalizzato all'esercizio di: - pedopornografia: ogni rappresentazione, con qualunque mezzo, di un minore in attività sessuali specifiche, reali

o simulate, o qualunque rappresentazione degli organi sessuali di un minore per scopi principalmente sessuali, - prostituzione minorile: il minore viene indotto a compiere atti sessuali in cambio di denaro o altra utilità; - turismo sessuale: si definisce "turista sessuale" colui che al fine di praticare sesso con i minori, organizza periodi di vacanza (o di lavoro) in paesi che, non solo tollerano la prostituzione minorile, ma spesso la propagandano per attirare il turista e incassare così valuta pregiata.

Abuso "on line"

Per abuso "on line" si intende ogni forma di abuso sessuale su minori perpetrata attraverso internet e la documentazione di immagini, video, registrazioni di attività sessuali esplicite, reali o simulate. L'abuso può prendere l'avvio da diverse situazioni: a) adescamento su internet con lo scopo di un coinvolgimento in attività di cibersex (sesso virtuale); b) induzione a guardare pornografia per adulti, induzione alla produzione di foto o video erotiche ; c) adescamento su internet a scopo di incontri sessuali offline, con presenza o meno di materiale pedopornografico, per abuso offline per la produzione di materiale pedopornografico; d) servizi di sesso online o offline remunerati in seguito all'aggancio online. La rete permette la diffusione delle immagini in un enorme circuito telematico, l'accesso alle immagini dell'abuso da parte di molte persone e la possibilità di scaricarle. Il fatto che la "realtà" dell'abuso si cristallizza nella rete, distorcendo la dimensione temporale dei fatti, unito alle conseguenze della vittimizzazione sessuale in un soggetto in età evolutiva, lo caratterizza come un "trauma pervasivo": le immagini dell'abuso o dei contatti sessuali in rete amplificano all'infinito gli effetti dell'abuso sulla vittima, l'abuso diventa, così, una realtà fattuale persecutoria ed eterna con cui la vittima deve fare i conti "per sempre".

9

INDICAZIONE METODOLOGICA

La scelta di avvalersi dello strumento dell'Equipe Multidisciplinare, in tempi brevissimi e formalizzati risponde all'esigenza di adottare una prospettiva integrata e condivisa tra diverse professionalità e servizi, così da garantire la maggiore appropriatezza possibile ai percorsi attivati.

È noto che ai sensi e per gli effetti degli artt. 357, 358 e 362 c.p. i pubblici ufficiali e gli incaricati di pubblico servizio hanno l'obbligo di denunciare la notizia di reato all'Autorità Giudiziaria in presenza di reati procedibili d'ufficio (ossia in presenza di reati per i quali la legge penale non prevede come necessaria la querela della persona offesa).

Il personale docente e in generale il personale scolastico assolve l'obbligo in questione 'riferendo' la notizia di reato di cui sono venuti a conos cenza al Dirigente scolastico, posto che soltanto ad esso spetta la competenza di rappresentanza legale e di relazione con l'esterno.

A fronte del quadro normativo di riferimento, è utile sottolineare come le situazioni di pregiudizio che possano configurare elementi di reato perseguibile d'ufficio non sempre

presentino elementi chiari e di facile rilevazione. I soggetti che impattano in situazioni di violenza e sofferenza possono sviluppare dubbi, vissuti emotivi di malessere, idiosincrasie che, se non adeguatamente gestiti, hanno l'effetto di ostacolare l'attivazione di un percorso efficace destinato ai minorenni coinvolti.

In questo scenario l'Equipe Multidisciplinare si pone come cornice tutelante rivolta in primis alle vittime, ma necessaria anche a tutti gli operatori della rete coinvolti nell'approntare e qualificare interventi complessi contrassegnati da rilevanti risvolti emotivi.

10

TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'art. 13 del Regolamento UE 679/16 ("GDPR"), i dati personali forniti sono raccolti unicamente per la seguente finalità: progetto "La Rete Si-cura" , che ne rappresenta la base giuridica di trattamento.

Nell'ambito del trattamento dei dati personali in esecuzione al presente progetto, l'Azienda Sociale Comuni Insieme, i Comuni dell'Ambito di Lomazzo-Fino Mornasco e gli Istituti Comprensivi dell'Ambito di Lomazzo-Fino Mornasco si impegnano a mantenere la massima riservatezza con riferimento al trattamento dei dati personali, dati particolari ("sensibili") ai sensi art. 9 del GDPR e giudiziari ai sensi art. 10 del GDPR, in ottemperanza al Regolamento UE 679/16 ("GDPR") mediante l'adozione, ciascuno per quanto di propria competenza, delle adeguate misure tecniche e organizzative per la sicurezza del trattamento ai sensi dell'art. 32 del Regolamento UE 679/16.

I Contitolari del Trattamento dei dati personali ai sensi dell'art. 26 del Regolamento UE 679/16 per il presente progetto "La Rete Si-cura" sono L'Azienda Sociale Comuni Insieme, i Comuni dell'Ambito di Lomazzo-Fino Mornasco e gli Istituti Comprensivi dell'Ambito di Lomazzo-Fino Mornasco.

L'Azienda Sociale Comuni Insieme, i Comuni dell'Ambito di Lomazzo-Fino Mornasco e gli Istituti Comprensivi dell'Ambito di Lomazzo-Fino Mornasco ciascuno nell'ambito della propria competenza e perimetro di attività, sono tenuti a provvedere alla formalizzazione degli atti di nomina dei Responsabili interni ed esterni, gli Incaricati Autorizzati che operano nell'ambito del progetto e trattato i dati personali , particolari e giudiziari, nonché formalizzare la nomina dei propri Responsabili per la Protezione Dati (DPO) ai sensi art. 37- 38 e 39 del Regolamento UE 679/16.

I diritti spettanti all'interessato in relazione al trattamento dei propri dati sono previsti dagli articoli da 15 a 21 del Regolamento UE 679/16 sono: diritto di accesso, diritto di rettifica, diritto alla cancellazione, diritto di limitazione al trattamento, obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento, diritto di opposizione.

11

DICHIARAZIONE D'INTENTI

Le presenti Linee Guida intendono portare a sistema l'impegno congiunto per l'adozione di una procedura condivisa per l'efficace gestione in rete di situazioni di maltrattamento e violenza assistita familiare a danno di minorenni di cui emerge notizia negli Istituti Comprensivi dell'Ambito Territoriale Sociale di Lomazzo – Fino Mornasco.

Sono regolati pertanto dal presente documento gli interventi che, svolti in collaborazione tra i soggetti firmatari, ricadono sui rispettivi sistemi di riferimento.

Le parti firmatarie del presente documento concordano in via sperimentale di operare in modo integrato in ottemperanza alle Linee Guida descritte.

Tutti i firmatari e i soggetti coinvolti all'interno dell'Equipe Multidisciplin are si impegnano a mantenere segretezza sui fatti di cui vengono a conoscenza .

È prevista la possibilità:

• di integrare le presenti Linee Guida con ulteriori elaborati tecnici, sulla base di specifiche esigenze che saranno concordate tra le parti;

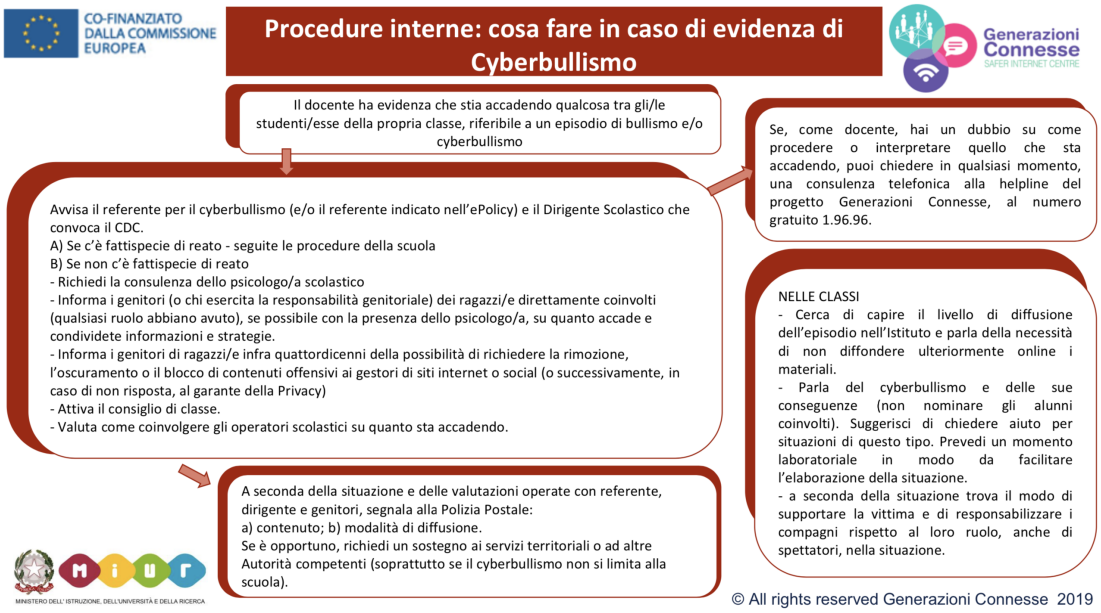
• di integrare le presenti linee guida con ulteriori soggetti aderenti, in base ad accordi che saranno assunti tra le parti;

• di modificare e/o integrare gli impegni assunti con la normativa vigente.

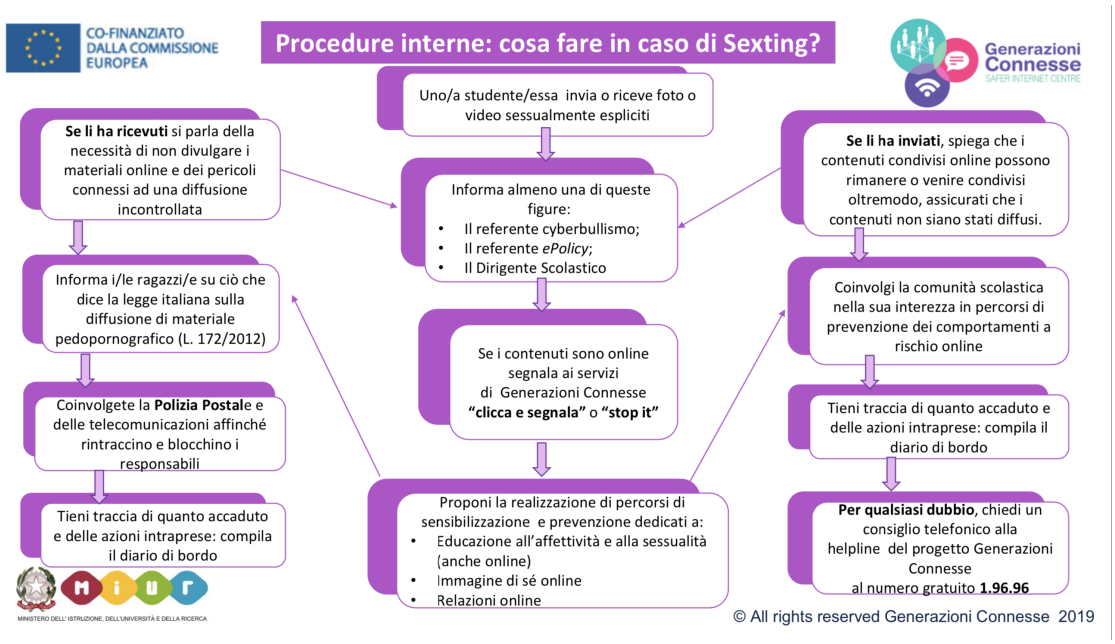
La validità del presente documento decorre dalla sua sottoscrizione con scadenza 31.12.2020.

5.4. - Allegati con le procedure

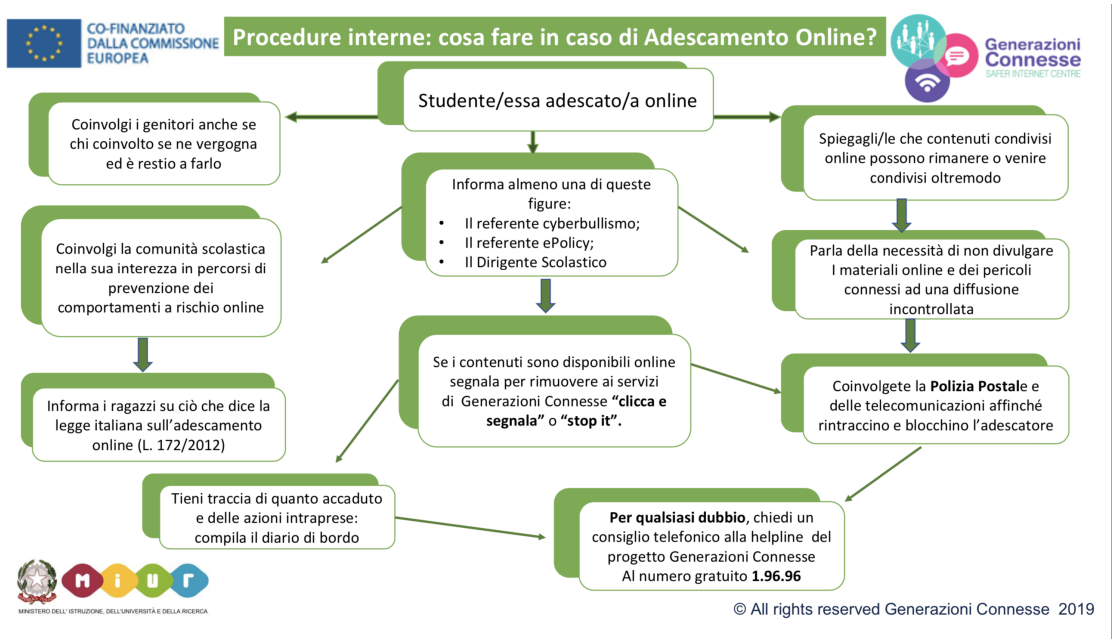
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



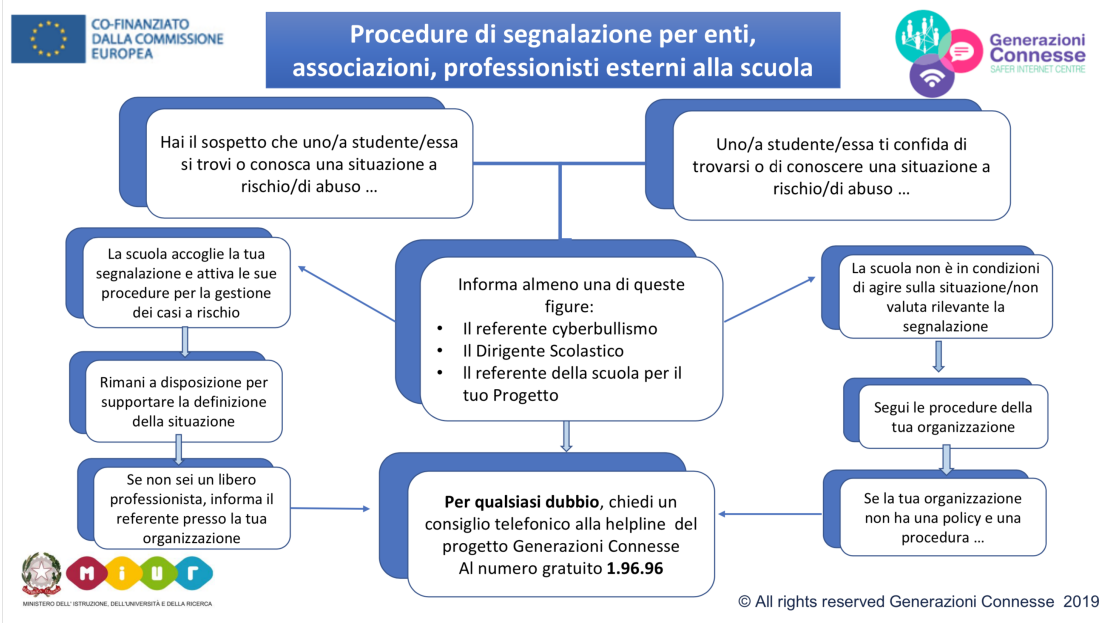
Procedure interne: cosa fare in caso di sexting?



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

- Informare docenti, studenti e famiglie in merito alle procedure e agli strumenti di segnalazione.
- Creare e sostenere una rete territoriale di supporto per la gestione integrata dei casi.

Firmato digitalmente da:

ILDOS ANGELA SERENA

Firmato il 28/10/2020 18:20

Seriale Certificato: 19008729

Valido dal 30/06/2020 al 30/06/2023

InfoCert Firma Qualificata 2