



Istituto Comprensivo Statale "Koiné"

Scuola dell'Infanzia, Primaria e Secondaria di primo grado  
via Gentili, 20 - 20900 Monza (MB) tel. e fax: 0392000621

e-mail: [mbic8ah00d@istruzione.it](mailto:mbic8ah00d@istruzione.it) [mbic8ah00d@pec.istruzione.it](mailto:mbic8ah00d@pec.istruzione.it) cod. fis. 94581300152  
codice univoco dell'ufficio: UFPQH9



## ***E-Safety Policy***

***a.s 2020/21***



## **PROPOSTA A TUTTA LA COMUNITÀ SCOLASTICA (studenti, genitori, docenti e personale ata)**

### **e-Safety Policy INDICE RAGIONATO**

#### 1. INTRODUZIONE

- 1.1 Scopo della Policy.
- 1.2 Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica).
- 1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica.
- 1.4 Gestione delle infrazioni alla Policy.
- 1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento.
- 1.6 Integrazione della Policy con Regolamenti esistenti.

#### 2. FORMAZIONE E CURRICOLO

- 2.1 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
- 2.2 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

#### 3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA SCUOLA

- 3.1 Accesso ad Internet: filtri antivirus e sulla navigazione.
- 3.2 Gestione accessi (password, backup, ecc.).
- 3.3 E-mail.
- 3.4 Blog e sito web della scuola
- 3.5 Social network.
- 3.6 Registro elettronico
- 3.7 Protezione dei dati personali.

#### 4. STRUMENTAZIONE DEL PERSONALE

- 4.1 Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc...
- 4.2 Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc...
- 4.3 Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc...

#### 5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

- 5.1 Prevenzione
  - Rischi e Azioni
- 5.2 Sportello d'ascolto
- 5.3 Rilevazione
  - 5.3.1 *Come segnalare*: procedure operative e strumenti
    - Procedure operative in caso di sospetto o evidente caso di cyberbullismo
    - Gli strumenti per segnalare e monitorare i casi a scuola
  - 5.3.2 *Come gestire le segnalazioni*
    - il numero verde 1.96.96 e i servizi di ascolto e segnalazione
    - cosa succede quando segnali
- 5.4 Come gestire i casi
  - 5.4.1 Procedura per casi gravi di cyberbullismo
  - 5.4.2 Nuovi strumenti della L. 71/2017: l'ammonimento
- 5.5 Azioni disciplinari di infrazioni accertate

## ALLEGATI

1. ALLEGATO 1 Strumenti per la segnalazione
2. ALLEGATO 2 Diario di bordo
3. ALLEGATO 3 Schema di procedimento per i casi sospetti di cyberbullismo
4. ALLEGATO 4 Schema di procedimento per i casi accertati di cyberbullismo
5. ALLEGATO 5 Schema di procedimento per i casi sexting
6. ALLEGATO 6 Modello di segnalazione per il garante per la protezione dei dati personali
7. Linee guida per i ragazzi
8. Linee guida per i genitori
9. Linee guida per gli insegnanti

## 1. INTRODUZIONE

*Nell'ambito del progetto "Generazioni connesse" ([www.generazioniconnesse.it](http://www.generazioniconnesse.it)), l'Istituto Comprensivo Koinè di Monza, nell'organo del team antibullismo, predispone questo documento programma anche in conformità con le LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo (aprile 2015 e aggiornamento ottobre 2017) elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con il Safer Internet Center per l'Italia, programma comunitario istituito dal Parlamento Europeo e dal Consiglio dell'Unione. Non si tratta di un documento meramente formale, poiché a partire da esso la scuola intende promuovere:*

- *la formazione rivolta al personale interno circa le tematiche previste dalla policy;*
- *l'impegno di tutti gli attori coinvolti nel rispetto di quanto definito nel documento;*
- *l'adeguamento del curricolo per ottemperare a quanto stabilito nella policy;*
- *la sensibilizzazione dei genitori sul tema della sicurezza online;*
- *dei partenariati con enti e associazioni esterne.*

*Internet è un'inestimabile risorsa per l'educazione e l'informazione, offre infinite opportunità per fare ricerca, comunicare, documentare il proprio lavoro, pubblicare elaborati e mettere in comune esperienze. Da un punto di vista amministrativo, grazie all'implementazione costante del sito internet della scuola, all'introduzione del registro elettronico e all'utilizzo della piattaforme web Axios e Weschool, a cui possono accedere Dirigente, docenti, genitori, alunni e personale amministrativo, è diventato più semplice gestire il sistema-scuola e aprire la scuola all'utenza con una comunicazione più tempestiva, chiara e trasparente.*

*Allo stesso tempo, l'uso sempre più pervasivo di piattaforme in rete e dispositivi portatili ha esposto gli utenti e in particolare i minori, i soggetti con divario digitale o con limitate competenze informatiche a nuovi rischi, tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usare la rete e alla consapevolezza delle funzioni rese possibili.*

*L'obiettivo è quello di educare e sensibilizzare gli adolescenti, gli insegnanti e i genitori all'uso sicuro e consapevole di internet. Soprattutto a seguito dell'emergenza Covid intervenuta a partire dalla fine del mese di febbraio 2020 e sino alla data odierna, l'Istituto si è trovato improvvisamente impegnato nella pratica della Didattica a Distanza e della Didattica digitale Integrata; questa esperienza ha reso evidenti alcune urgenze organizzative, formative e didattiche relative alle competenze digitali dei ragazzi e degli adulti coinvolti nel processo educativo.*

**Definizione di cyberbullismo:** *"Bullismo telematico è qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo". (L. 71/2017)*

*A questo si aggiunge che per forma di cyberbullismo la scuola, intende anche la diffusione di contenuti online da parte di alunni con lo scopo di diffamare, denigrare, offendere, alterare, manipolare la persona o l'operato di docenti, personale scolastico, collaboratori Ata, educatori e tutti quelli che fanno parte della formazione ed educazione all'interno del nostro Istituto Comprensivo Koinè di Monza.*

*Pertanto la nostra Scuola ha deciso di sviluppare e attuare il progetto "Generazioni Connesse"*

([www.generazioniconnesse.it](http://www.generazioniconnesse.it)) attraverso la realizzazione di due linee di intervento:

1. l'elaborazione di linee guida per una eSafety Policy d'Istituto, cioè di un proprio codice di condotta nella prevenzione e gestione dei casi di (cyber)bullismo e di un regolamento di sicurezza informatica che ha preso come riferimento i principi proposti dal MIUR nel documento che riassume "La posizione italiana sui principi fondamentali di Internet";
2. la cittadinanza digitale con la promozione nei confronti degli alunni della competenza digitale e della cultura del rispetto di regole comuni nell'uso dei servizi telematici e lo sviluppo di regole di buon comportamento (Netiquette) riferite specialmente ai Social Network e della conoscenza delle condizioni del loro utilizzo.

### **1.1 Scopo della Policy**

Lo scopo della e-Safety Policy è di condividere e stabilire con tutti i membri della comunità scolastica regole, modalità e principi sull'utilizzo consapevole e corretto di internet.

In particolare, essa viene redatta per regolare il comportamento della componente studentesca dentro le aule scolastiche e per sensibilizzarli all'adozione di buone pratiche quando sono fuori dalla scuola. Questo è il caso degli episodi di cyberbullismo come di altri fenomeni di cui si tratta nella presente politica, che possono avvenire al di fuori della scuola, ma che sono legati alla frequentazione della stessa.

Il nostro Istituto accoglie minori "nativi digitali" che fin dalla scuola primaria sono esposti a rischi di cui sono inconsapevoli, pertanto la scuola attua, parallelamente, attività di prevenzione, controllo e formazione di allieve, allievi e famiglie allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità scolastica, ma possono configurarsi come reati.

La scuola opererà, eventualmente, in stretto collegamento con le forze dell'ordine e con le istituzioni del settore educativo, per mettere in campo strategie di prevenzione al cyberbullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.

Le indicazioni, contenute nella presente e-Safety Policy, intendono dare al nostro Istituto un impulso allo sviluppo di una cultura d'uso corretto e consapevole di Internet, sia tramite il richiamo a norme vigenti, sia con l'indicazione di prassi e protocolli operativi opportuni per un uso sempre più professionale da parte di tutto il personale e per la prevenzione dei rischi e la gestione delle emergenze.

I principi fondamentali richiamati sono:

- salvaguardare e proteggere i bambini, i ragazzi e tutto il personale dell'Istituto;
- assistere il personale della scuola a lavorare in modo sicuro e responsabile con le tecnologie di comunicazione di Internet e monitorare i propri standard e le proprie prassi didattiche e di comunicazione interna alla scuola;
- impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo;
- adottare un protocollo di intervento per rilevare, monitorare e gestire gli abusi online come il cyberbullismo, che sono riferimenti incrociati con le altre politiche della scuola;
- garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie.

Gli utenti, siano essi maggiorenni o minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. *La presente policy sarà parte integrante del Regolamento di Istituto, alla sua stesura saranno coinvolti genitori, alunni e tutto il personale*

della scuola, e portato a conoscenza degli Organi Collegiali e di tutti gli operatori e gli utenti della scuola; con questo atto si intende attivare e mantenere nella nostra scuola una eSafety Policy in materia di tecnologie dell'informazione e della comunicazione condivisa e accettata da tutti.

## **1.2 Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica).**

<p><b>1. Dirigente scolastico</b>          Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti:</p>	<ul style="list-style-type: none"> <li>• Elabora, in collaborazione con il/i referente/i per il bullismo e il cyberbullismo, nell'ambito dell'autonomia del proprio istituto, un Regolamento condiviso per il contrasto dei fenomeni di bullismo e cyberbullismo, che preveda sanzioni in un'ottica di giustizia riparativa e forme di supporto alle vittime. Il Regolamento deve essere esplicitato nel Patto di corresponsabilità educativa firmato dai genitori. i contenuti del Regolamento vanno condivisi e approvati dal Consiglio d'istituto.</li> <li>• Promuove interventi di prevenzione primaria e per le scuole secondarie sollecita il coinvolgimento attivo degli studenti anche attraverso modalità di peer education.</li> <li>• Organizza e coordina i Team Antibullismo e per l'Emergenza.</li> <li>• Predisporre eventuali piani di sorveglianza in funzione delle necessità della scuola.</li> <li>• Tramite il sito web della scuola si forniscono le seguenti informazioni:             <ul style="list-style-type: none"> <li>-nominativo/i del/i referente/i per il bullismo e cyberbullismo;</li> <li>- contenuti informativi su azioni e attività di contrasto ai fenomeni di bullismo e cyberbullismo (Regolamento d'istituto, PTOF, Patto di corresponsabilità) oltre che di educazione digitale.</li> </ul> </li> </ul>
<p><b>2. Il Consiglio di Istituto</b></p>	<ul style="list-style-type: none"> <li>• Approva il Regolamento d'istituto, che deve contenere possibili azioni sanzionatorie e/o riparative in caso di bullismo e cyberbullismo.</li> <li>• Facilita la promozione del Patto di corresponsabilità tra scuola e famiglia.</li> </ul>
<p><b>3. Il Collegio dei docenti</b></p>	<ul style="list-style-type: none"> <li>• All'interno del PTOF e del Patto di corresponsabilità predispone azioni e attività per la prevenzione dei fenomeni di bullismo e cyberbullismo, comprensive delle azioni di prevenzione primaria/universale specifiche per ogni ordine di scuola e delle azioni indicate rivolte a prendere in carico le situazioni di emergenza nella scuola. In modo particolare, organizza attività di formazione rivolte agli studenti sulle tematiche di bullismo, cyberbullismo ed educazione digitale</li> <li>• In relazione alle situazioni di emergenza, approva i protocolli di segnalazione e intervento promossi dal</li> </ul>

	<p>Team Antibullismo della scuola e collabora attivamente con il Team e le altre agenzie per la soluzione dei problemi</p> <ul style="list-style-type: none"> <li>• Predispone gli obiettivi nell'area educativa, per prevenire e contrastare il bullismo e il cyberbullismo attraverso attività di curriculum scolastico. In tal senso, è importante legare la progettazione della scuola in una ottica di prevenzione dei fenomeni di bullismo e cyberbullismo riferendosi a quanto previsto con la L. 92/2019 "Introduzione dell'insegnamento dell'Educazione civica", in particolare all'art. 3 "Sviluppo delle competenze e obiettivi di apprendimento" e all'art. 5 "Educazione alla cittadinanza digitale".</li> <li>• Partecipa alle attività di formazione per il contrasto dei fenomeni di bullismo e cyberbullismo organizzate da ogni autonomia scolastica, eventualmente avvalendosi di attività offerte da servizi istituzionali o enti qualificati presenti sul territorio (si vd. quanto proposto sulla piattaforma ELISA - <a href="http://www.piattaformaelisa.it">www.piattaformaelisa.it</a>)</li> </ul>
<b>4. Animatore digitale</b>	<ul style="list-style-type: none"> <li>- Stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;</li> <li>- Si relaziona con la ditta che gestisce l'assistenza tecnico-informatica per definire le misure di sicurezza informatica più opportune</li> <li>- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;</li> <li>- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curarne la manutenzione;</li> <li>- condividere la E-Safety Policy sul sito della scuola;</li> <li>- controllo (una tantum e/o all'evenienza di episodi dubbi) del sistema informatico (cronologia, cookies, ecc.) da parte dei responsabili;</li> <li>- installazione di firewall sull'accesso Internet;</li> <li>- aggiornamento periodico del software antivirus e scansione delle macchine in caso di sospetta presenza di virus.</li> </ul>
<b>5. DSGA</b>	<ul style="list-style-type: none"> <li>- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;</li> <li>- garantire il funzionamento dei diversi canali di</li> </ul>

	<p>comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.</p>
<p>6. I Coordinatori dei Consigli di Classe</p>	<ul style="list-style-type: none"> <li>• Monitorano che vengano misurati gli obiettivi dell'area educativa, attivando le procedure anti bullismo.</li> <li>• Registrano nei verbali del Consiglio di classe: casi di bullismo, comminazione delle sanzioni deliberate, attività di recupero, collaborazioni con pedagogo, psicologo, forze dell'ordine specializzate nell'intervento per il bullismo e il cyberbullismo, enti del territorio in rete (con riferimento e coordinamento eventuale da parte delle prefetture).</li> </ul>
<p><b>7. Referente per il bullismo</b></p>	<ul style="list-style-type: none"> <li>• Collabora con gli insegnanti della scuola, propone corsi di formazione al Collegio dei docenti, coadiuva il Dirigente scolastico nella redazione dei Piani di vigilanza attiva ai fini della prevenzione degli episodi di bullismo e di cyberbullismo, monitora i casi di bullismo e cyberbullismo, coordina i Team Antibullismo e per l'Emergenza, crea alleanze con il Referente territoriale e regionale, coinvolge in un'azione di collaborazione Enti del territorio in rete (psicologi, forze dell'ordine, assistenti sociali, pedagogisti, ecc.)</li> </ul>
<p><b>8. I Referenti degli Uffici scolastici regionali e territoriali per il bullismo e il cyber bullismo</b></p>	<ul style="list-style-type: none"> <li>• Forniscono, attraverso la pagina web istituzionale, a tutti i Referenti d'istituto informazioni sui corsi di formazione. Agevolano la messa in rete dei Referenti di ogni singola scuola.</li> <li>• Collaborano per i livelli di competenza (regionale e provinciale), con la Polizia postale, con i Carabinieri, con gli Enti del territorio e con il MI.</li> <li>• Partecipano a specifici corsi di formazione e agevolano l'azione di filiera tra scuola ed extra scuola e tra la scuola e la Direzione generale per lo studente del MI</li> <li>• Collaborano inoltre con i Referenti regionali delle Consulte provinciali degli studenti, dell'Associazione regionale dei genitori (Forags) e del Piano nazionale scuola digitale (PNSD).</li> </ul>
<p><b>9. I TEAM ANTIBULLISMO E PER L'EMERGENZA (scuola primaria e secondaria di primo e secondo grado)</b></p>	<ul style="list-style-type: none"> <li>• Coordinano e organizzano attività di prevenzione. Intervengono nei casi acuti.</li> <li>• Comunicano al Referente regionale (anche tramite i Referenti territoriali), alla fine di ogni anno scolastico, i casi di bullismo o cyberbullismo. I dati serviranno per un eventuale monitoraggio nazionale dei fenomeni di bullismo e cyberbullismo e potranno essere trasmessi dai Referenti regionali alla Commissione nazionale istituita presso il Ministero dell'Istruzione.</li> </ul>

<p><b>10. Il personale scolastico (ata, segreterie, etc)</b></p>	<ul style="list-style-type: none"> <li>• Svolgono un ruolo di vigilanza attiva nelle aree dove si svolgono gli intervalli, nelle mense, negli spogliatoi delle palestre, negli spazi esterni, al cambio dell'ora di lezione e durante i viaggi di istruzione, ferme restando le responsabilità dei docenti. Nella scuola secondaria di secondo grado, faranno parte dei Piani di vigilanza attiva anche gli Assistenti Tecnici che svolgono la loro attività in laboratorio.</li> <li>• Partecipano alle attività di formazione per il bullismo e il cyberbullismo organizzate dalla scuola.</li> <li>• Segnalano al dirigente scolastico e ai Team Antibullismo e per l'Emergenza eventuali episodi o comportamenti di bullismo e cyberbullismo di cui vengono a conoscenza direttamente e/o indirettamente.</li> <li>• Se dovessero intervenire per bloccare eventuali comportamenti di bullismo in essere, lo faranno applicando le modalità previste dal Regolamento d'Istituto.</li> <li>• Aver letto, compreso e sottoscritto la seguente policy.</li> </ul>
<p><b>11. I Docenti</b> Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:</p>	<ul style="list-style-type: none"> <li>- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;</li> <li>- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;</li> <li>- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;</li> <li>- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;</li> <li>- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali, quindi non private;</li> <li>- evitare partecipazione a gruppi di condivisione di Whatsapp o altro, inerenti alla scuola (gruppi classe, gruppi genitori, etc..), se non autorizzati dal/la Dirigente;</li> <li>- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;</li> <li>- tutti i docenti, venuti a conoscenza diretta o indiretta di eventuali episodi di bullismo o cyber bullismo, sono chiamati a segnalarli al referente scolastico o al team</li> </ul>

	<p>antibullismo di Istituto, al fine di avviare una strategia di intervento concordata e tempestiva.</p> <ul style="list-style-type: none"> <li>- Gli insegnanti sono responsabili delle TIC nell'ambito dell'attività didattica e hanno il compito di responsabilizzare gli alunni per divenire consapevoli dell'importanza della salvaguardia di un bene comune, seguendo le corrette norme di utilizzo.</li> <li>- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);</li> <li>- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;</li> <li>- comunicare al referente sul bullismo e alla Dirigente scolastica, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;</li> <li>- presenza di un docente o di un adulto responsabile durante l'utilizzo di Internet, della piattaforma o di altre tecnologie I.C., da parte dei ragazzi;</li> <li>- attenzione all'utilizzo di penne USB, CD/DVD o altri dispositivi esterni personali e dell'istituto;</li> <li>- dare chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli alunni la netiquette e indicandone le regole;</li> <li>- non divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete wifi;</li> <li>- non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione;</li> <li>- non salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;</li> <li>- proporre agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento;</li> <li>- illustrare ai propri alunni le regole di utilizzo contenute nel presente documento;</li> <li>- aver letto, compreso e sottoscritto la presente policy;</li> </ul>
--	---

<p><b>12. Le studentesse e gli studenti</b></p>	<ul style="list-style-type: none"> <li>- Partecipano alle attività di prevenzione del bullismo e del cyberbullismo organizzate dalla scuola</li> <li>- Sono chiamati a essere parte attiva nelle azioni di contrasto al bullismo e al cyberbullismo e di tutela della vittima, riferendo ai docenti e agli altri adulti gli episodi e i comportamenti di bullismo e cyberbullismo di cui vengono a conoscenza e supportando il/la compagno/a vittima (consolandola e intervenendo attivamente in sua difesa). Nella scuola secondaria di primo e secondo grado sono chiamati a collaborare alla realizzazione di attività di peer education. L'istituzione scolastica può favorire percorsi specifici in merito alla formazione dei rappresentanti degli studenti negli organi collegiali.</li> <li>- accettare la e-safety policy;</li> </ul>
<p><b>13. Le famiglie</b></p>	<ul style="list-style-type: none"> <li>• Sono invitate a partecipare agli incontri di informazione e sensibilizzazione sui fenomeni di bullismo e cyberbullismo, favorendo una proficua alleanza educativa.</li> <li>• Firmano il patto di corresponsabilità educativa scuola-famiglia.</li> <li>• In questo contesto i genitori devono essere informati sul Regolamento d'istituto, sulle misure prese dalla scuola e sulle potenziali implicazioni penali e civili per il minore e per la famiglia come conseguenza di atti di bullismo e cyberbullismo</li> <li>• Sono chiamate a collaborare con la scuola nella prevenzione del bullismo e nelle azioni per fronteggiare le situazioni acute.</li> </ul>

### 1.3 Condivisione e comunicazione della policy all'intera comunità scolastica

L'Istituto si impegna a diffondere la presente policy per condividerne i contenuti con tutta la comunità scolastica.

La Policy sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- pubblicazione della E-Safety Policy sul sito della scuola;
- accordo di utilizzo accettabile, discusso con gli studenti e i genitori, all'inizio dell'anno, **tramite il Patto di Corresponsabilità**, che sarà sottoscritto dalle famiglie e rilasciato alle stesse;
- accordo di utilizzo accettabile rilasciato al personale scolastico.

Inoltre, si ricorda che nella legge 20 agosto 2019 n. 92 "Introduzione dell'insegnamento scolastico dell'educazione civica" prevede, fra l'altro, nell'ambito dell'insegnamento trasversale dell'educazione civica, l'educazione alla cittadinanza digitale.

Successivamente si condividerà nelle seguenti modalità a seconda degli attori interessati per raggiungere in modo più incisivo le singole parti:

- a) La condivisione e comunicazione della politica di e-safety **alle studentesse e studenti:**
  - Attraverso la discussione in classe della policy nei primi giorni di scuola, con particolare

riguardo al protocollo di utilizzo di internet per le nuove classi prime;

- Istruire e informare gli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete;
- Sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.
- La scuola promuoverà eventi e/o dibattiti informativi e formativi, in momenti diversi dell'anno, rivolti a tutto il personale, agli alunni e ai loro genitori, con il coinvolgimento di esperti, sui temi oggetto di codesto Documento.
- Tra le misure di prevenzione che la scuola metterà in atto ci saranno, inoltre, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze così che l'utilizzo di Internet e dei cellulari oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di trasparenza i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni. A tal proposito si manterrà l'attivazione di uno "Sportello di ascolto" rivolto a tutti gli alunni, articolato in colloqui individuali e/o collettivi, al fine di migliorare il benessere personale e scolastico mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale. Si prevede al suo interno, anche uno spazio riservato ai docenti e genitori al fine di individuare strategie efficaci per affrontare problematiche tipiche dell'età adolescenziale.

**b) La condivisione e comunicazione della politica di e-safety al personale:**

- La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali (consigli di interclasse/intersezione, collegio dei docenti) e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;
- Per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;
- Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;
- Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.
- un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente;
- elaborazione di protocolli condivisi di intervento.

**c) La condivisione e comunicazione della politica di e-safety alle famiglie:**

- L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree del sito web della scuola;
- Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;
- La scuola fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa;
- l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.
- Allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a

scuola, si invitano tutti i genitori a prestare la massima attenzione ai principi e alle regole contenute nel presente documento.

#### **1.4 Gestione delle infrazioni alla policy**

Le infrazioni alla policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA, referenti cyberbullismo, vicario della Dirigente e al Dirigente scolastico stesso.

Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso.

Il Dirigente scolastico ha la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (pc, tablet, notebook, ecc...) a chi non si attiene alle regole stabilite.

La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line. Tuttavia, a causa della scala internazionale collegata ai contenuti Internet, la disponibilità di tecnologie mobili e velocità di cambiamento, non è possibile garantire che il materiale non idoneo apparirà mai su un computer della scuola o dispositivo mobile.

Né la scuola né l'autorità locale possono accettare la responsabilità per il materiale accessibile, o le conseguenze di accesso a Internet.

Al personale e agli alunni saranno date informazioni sulle infrazioni in uso e le eventuali sanzioni contenute nel Regolamento di Istituto o nel presente documento. Nel caso in cui le infrazioni della policy violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.

Nelle sezioni successive al presente documento sono, inoltre, richiamate e specificate le infrazioni e relative sanzioni.

I provvedimenti includono:

- ✓ Qualsiasi rilevamento di sospetto abuso, offesa, procurato disagio ricevuto su internet, sia personale che di un compagno, sarà sempre riferito, da parte del personale scolastico, al Dirigente Scolastico e al referente del bullismo che fungeranno da primo punto di contatto;
- ✓ Possibile ritiro del cellulare fino a fine giornata;
- ✓ Saranno informati e documentati i genitori o i tutori per condividere con loro le strategie più opportune;
- ✓ Denunce di bullismo online saranno trattate in conformità con la legge attuale.  
Reclami relativi alla protezione dei bambini saranno trattati in conformità alle procedure di protezione dell'infanzia;
- ✓ Nei casi più gravi, saranno avviate le comunicazioni alle autorità competenti;
- ✓ Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso.  
Infatti, è bene ricordare a tutti che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia.

#### **1) Disciplina degli studenti e delle studentesse**

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle

tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

1. un uso della rete per giudicare, infastidire o impedire, in modo persistente, a qualcuno di esprimersi o partecipare;
2. l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
3. l'invio o la condivisione di immagini intime o troppo spinte;
4. il collegamento a siti web, nell'orario scolastico, non autorizzati dai docenti.
5. L'utilizzo, non autorizzato o comunicato ai docenti, dello smartphone in orario scolastico (utilizzando messaggiera, video, audio o foto).

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

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

## 2) Disciplina del personale scolastico

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

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conformi ai principi della privacy o che non garantisce un'adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

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

Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o

della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

### 3) Disciplina delle famiglie

Le famiglie delle studentesse e degli studenti possono essere convocate a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

## **1.5 Monitoraggio dell'implementazione della policy e suo aggiornamento**

La E-Safety Policy si inserisce all'interno di altre politiche scolastiche, quali la politica di protezione dei minori, la politica antibullismo, la politica del benessere degli alunni a scuola. Come già ricordato, la E-Safety Policy sarà riesaminata annualmente o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e tutte le modifiche della Policy saranno discusse in dettaglio con tutti i membri del personale docente.

- Nell'ambito del monitoraggio dell'implementazione della E-Safety Policy si terranno in considerazione i dati annuali sulla base del seguente documento:

ANNO SCOLASTICO	NUMERO Di segnalazioni	NUMERO Di infrazioni	NUMERO Di sanzioni disciplinari

## **1.6 Integrazione della policy con i regolamenti esistenti**

La presente e-policy safety o regolamento per l'uso delle risorse tecnologiche e di rete è stato allegato al Regolamento di Istituto e inserito nel sito web della scuola.

I genitori vengono informati della pubblicazione del presente "Regolamento per l'uso delle risorse tecnologiche e di rete" della scuola e possono prenderne visione sul sito della scuola.

## **2 FORMAZIONE E CURRICOLO**

Il nostro Istituto condivide le linee indicate nel Piano Nazionale Scuola Digitale (PNSD). Esse danno come indirizzo l'intento di modificare gli ambienti di apprendimento per rendere l'offerta formativa coerente con i cambiamenti della società della conoscenza e con le esigenze e gli stili cognitivi delle nuove generazioni.

Si ricorda il D.M. 851 del 27 ottobre 2015, in attuazione dell'art.1, comma 56 della legge 107/2015, che ne prevede l'attuazione al fine di:

- ✓ migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse;

- ✓ implementare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratoriali ivi presenti;
- ✓ favorire la formazione dei docenti sull'uso delle nuove tecnologie ai fini dell'innovazione didattica;
- ✓ individuare un Animatore Digitale ed un team per l'innovazione digitale che supporti ed accompagni adeguatamente l'innovazione didattica, nonché l'attività dell'animatore Digitale;
- ✓ partecipare a bandi nazionali ed europei per finanziare le suddette iniziative.

Tali indicazioni sono contenute anche nella legge 20 agosto 2019 n. 92 "Introduzione dell'insegnamento scolastico dell'educazione civica" che prevede, fra l'altro, nell'ambito dell'insegnamento trasversale dell'educazione civica, l'educazione alla cittadinanza digitale.

Inoltre, come previsto dalla L. 71/2017 e dall'aggiornamento delle "Linee di orientamento per la prevenzione e il contrasto del cyberbullismo" (nota MIUR prot. N. 5515 del 27-10-2017), Il Ministero dell'Istruzione si è impegnato nell'attuazione di un Piano Nazionale di Formazione dei docenti referenti per il contrasto al bullismo e al cyberbullismo.

## **2.1 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica**

La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno. A livello interno, nel PTOF si prevede che una parte della formazione in servizio sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione è svolta o da docenti dell'Istituto con formazione specifica o organizzando conferenze tenute da esperti esterni per permettere una adeguata formazione agli insegnanti stessi.

Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi.

## **2.2 Formazione dei docenti sull'utilizzo consapevole e sicuro di internet e delle tecnologie digitali**

La formazione in ingresso e in servizio è senza dubbio il cardine per assicurare l'adeguatezza della professionalità docente ai bisogni formativi ed educativi delle studentesse e degli studenti. Viste le positive reazioni di studenti, docenti e genitori e la necessità di implementare la eSafety Policy con il contributo di tutte le componenti, la Scuola continuerà ad organizzare per l'anno prossimo occasioni di confronto sulle strategie più opportune da adottare come promozione dell'utilizzo consapevole e sicuro di Internet e delle TIC e come misure di prevenzione primaria al (cyber)bullismo.

## **3 GESTIONE DELL'INFRASTRUTTURA, DELLA STRUMENTAZIONE TIC DELLA SCUOLA E DELLA STRUMENTAZIONE PERSONALE**

La scuola metterà in atto tutte le azioni necessarie per garantire agli studenti l'accesso alla documentazione cercata adottando tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio durante la navigazione.

Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti.

### **3.1 Accesso a internet (filtri, antivirus, navigazione)**

Il nostro Istituto ha configurato un proxy server per monitorare il traffico web e per bloccare l'accesso a siti inappropriati a un contesto scolastico.

Occorre, inoltre, sensibilizzare tutta la comunità scolastica sull'opportunità di mantenere aggiornati gli antivirus installati sulle macchine personali e controllare i dispositivi di archiviazione esterna che vengano collegati al proprio pc.

#### **Le principali norme sono:**

1. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;
2. Internet non può essere usato per scopi vietati dalla legislazione vigente;
3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;
4. È vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza. Consultare obbligatoriamente prima di installare qualsiasi programma l'animatore digitale, un responsabile di laboratorio o un tecnico per valutarne la compatibilità.

### **3.2 Gestione accessi (Password, backup, etc..)**

#### **Accesso docenti**

L'Istituto attualmente è dotato di una rete wireless destinata all' utilizzo didattico da parte del corpo docente.

La password è unica a livello di Istituto/plesso. Ai docenti è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto previa richiesta alla Dirigente o al suo vicario. Successivamente, le figure preposte, configurano il pc dell'interessato senza comunicare la password.

La scuola sta valutando, per tracciare gli utilizzi fatti della rete, la possibilità di abbinare l'ID del proprio PC ad accessi autorizzati registrando indirizzo rete di ogni pc e la sua corrispondente attività. Ciascun utente connesso alla rete dovrà rispettare il presente regolamento e la legislazione vigente succitata, tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso e rispettare la cosiddetta netiquette (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o e-mail).

La componente studentesca dovrà impegnarsi a rispettare le norme di buon utilizzo che la scuola ha elencato nel presente documento.

I computer portatili presenti nelle aule richiedono una password di accesso per l'accensione.

Ogni docente è quindi tenuto ad un controllo della strumentazione in aula poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante. Ogni docente accede al registro elettronico attraverso una password che non può essere comunicata a terzi, né agli alunni.

*Per quanto riguarda la connessione a internet si ricorda che:*

- ✓ *L'accesso può avvenire unicamente da tale dispositivo.*
- ✓ *Il proprietario del dispositivo è l'unico responsabile di tutte le operazioni svolte con esso.*
- ✓ *In caso di furto o smarrimento del dispositivo identificato si deve immediatamente informare il personale tecnico incaricato che ne revocherà l'accesso alla rete.*
- ✓ *Il docente verificherà lo spegnimento della postazione al termine della sua ora di lezione.*

#### **Accesso studenti**

#### **Il Regolamento di Istituto vieta l'uso del cellulare.**

In particolare, agli studenti **non** è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto.

È altresì vietato l'uso per scopo personale di tutti gli altri strumenti informatici di proprietà e non dello studente. L'eventuale utilizzo di strumenti informatici di proprietà dello studente durante l'attività didattica deve essere autorizzata dal docente.

Relativamente alle studentesse e studenti che accedono a Internet durante l'attività didattica sono consentiti la navigazione guidata da parte dell'insegnante e la stesura di documenti collaborativi purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato. E' vietato l'accesso alle chat-room pubbliche o non moderate. La trasgressione a queste regole avranno sanzione decisa dal Dirigente e dal CdC secondo le presenti norme e in accordo al Regolamento di Istituto.

### **3.3 E-mail**

Solo i docenti possono utilizzare i servizi mail accedendo alla rete della scuola a fini esclusivamente didattici.

Ogni docente possiede un account *nome.cognome@koinemonza.edu.it*.

L'account è strettamente personale, per cui ogni utente dovrà avere cura di disconnettere il proprio accesso al termine del suo utilizzo. Lo spazio è destinato alla ricezione di comunicazioni, all'invio di documentazione e alla condivisione di materiali, progetti didattici o progetti con altri docenti.

Sulla rete scolastica tutti sono invitati a utilizzare solo account di posta elettronica presenti nel dominio scolastico e per scopi inerenti allo svolgimento didattico/organizzativo.

Le comunicazioni tra personale scolastico, famiglie e studentesse/studenti via e-mail devono avvenire preferibilmente tramite un indirizzo e-mail della scuola (*-@koinemonza.edu.it*.) o all'interno della piattaforma di apprendimento weschool o tramite registro elettronico, per consentire l'attivazione di protocolli di controllo.

E-mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti.

### **3.4 Sito web della scuola**

Il Dirigente Scolastico e il personale incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato e appropriato.

La scuola offre all'interno del proprio sito una serie di servizi alle famiglie e ai fruitori esterni: i docenti che desiderano pubblicare attività didattiche dovranno chiedere l'autorizzazione al Dirigente.

Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato.

### **3.5 Social network (facebook, whatsapp, instagram,tiktok etc..) per studentesse e studenti, docenti e genitori/tutori.**

Per Legge l'utilizzo dei Social Network, con la pubblicazione di nomi e giudizi sulle persone o sulle istituzioni e la diffusione di foto/filmati senza il consenso all'insaputa delle persone coinvolte può determinare ricadute di carattere anche penale, come ad esempio la diffamazione.

Si invitano pertanto tutte le studentesse e tutti gli studenti a non prelevare o diffondere immagini, video o registrazioni – anche solo audio – non autorizzate, ed eliminare da internet eventuali riferimenti offensivi o comunque illeciti (ed inopportuni) nei confronti dell'Istituto e dei suoi docenti e studenti.

Allo stesso tempo, si invitano gli allievi e i genitori/tutori a fare un uso prudente dei Social Network, limitandone l'uso alle sole comunicazioni funzionali, evitando ad ogni modo di esprimere giudizi sull'operato degli altri studenti o del personale della scuola, giudizi che una volta pubblicati comportano sempre una assunzione di responsabilità da parte di chi li ha scritti o anche semplicemente diffusi.

Nella pratica didattica si cercherà di educare la componente studentesca al loro uso sicuro.

### **3.6 Registro elettronico**

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. L'uso del registro elettronico verrà spiegato alle famiglie nel corso di un incontro orientativo che si terrà alle famiglie all'apertura dell'anno scolastico oltre che ad alcune indicazioni guida da pubblicarsi sul sito della scuola. La pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante la studentessa/lo studente.

Coloro che non possono accedere a Internet, e di conseguenza non possono consultare il registro elettronico, sono pregati di darne segnalazione al coordinatore del consiglio di classe, che verificherà la trascrizione delle comunicazioni sul diario e la firma dei genitori/tutori.

### **3.7 Protezione dei dati personali**

Il 25 maggio 2018 è entrato in vigore in tutti gli stati aderenti all'Unione Europea il Regolamento del Parlamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, conosciuto come GDPR.

Anche se in parte quanto previsto dal nuovo Regolamento risulta facilmente sovrapponibile alla precedente normativa italiana, è però necessario ricordare che il GDPR diventa il nuovo riferimento per garantire la corretta tutela dei dati personali. Pertanto il nostro Istituto adeguerà le modalità e responsabilità opportune a questo documento.

Garantire la corretta tutela dei dati personali richiede, innanzitutto, l'individuazione dei dati trattati soggetti alla normativa vigente, nonché l'analisi delle modalità e responsabilità di gestione delle informazioni, onde identificare le eventuali criticità e gli adeguamenti da predisporre.

Saranno da individuare le misure di tutela attuate e da definire quelle da attuare, nonché le modalità per garantirne nel tempo la continuità e l'adeguatezza.

Dovranno inoltre essere stabilite le responsabilità per la gestione dei dati: titolare, responsabile, persone autorizzate al trattamento.

L'Istituto Comprensivo Koinè di Monza rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali che gli stessi conferiscono all'I.C. stesso. La raccolta ed il trattamento di dati personali avviene, quando necessario, in relazione all'esecuzione di servizi richiesti dall'utente, o quando l'utente stesso decide di comunicare i propri dati personali; in tali circostanze, la presente politica della privacy illustra le modalità ed i caratteri di raccolta e trattamento dei dati personali dell'utente. L'I.C. "Koinè" tratta i dati personali forniti dagli utenti in conformità alla normativa vigente.

In caso di raccolta di dati personali, l'I.C. "Koinè" informerà l'utente sulle finalità della raccolta al momento della stessa, ove necessario, richiederà il consenso dell'utente. L'Istituto non comunicherà i dati personali dell'utente a terzi senza il consenso dello stesso. Se l'utente decide di fornire alla scuola i propri dati personali, la scuola potrà comunicarli all'interno dell'Istituto od a terzi che prestano servizi alla scuola, solo rispetto a coloro che hanno bisogno di conoscerli

in ragione delle proprie mansioni, e, ove necessario, con il permesso dell'utente.

La scuola tratta i dati personali dell'utente per le seguenti finalità di carattere generale: per soddisfare le richieste a specifici prodotti o servizi, per personalizzare la visita dell'utente al sito, per aggiornare l'utente sulle ultime novità in relazione ai servizi offerti od altre informazioni che ritiene siano di interesse dell'utente che provengono direttamente dall'Istituto o dai suoi partners, e per comprendere meglio i bisogni dell'utente ed offrire allo stesso servizi migliori. Il trattamento di dati personali dell'utente da parte dell'Istituto, per le finalità sopra specificate avviene in conformità alla normativa vigente a tutela dei dati personali.

Infine, si fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c. d. Codice della Privacy). Tuttavia, si possono individuare al riguardo alcune linee guida di e- safety:

➤ Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione.  
Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet, e sui social network in particolare. (da vademecum privacy del Garante)

➤ In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video.

Si deve quindi prestare particolare attenzione prima di caricare immagini e video su blog o social network, oppure di diffonderle attraverso mms o sistemi di messaggistica istantanea. Succede spesso, tra l'altro, che una fotografia inviata a un amico o a un familiare venga poi inoltrata ad altri destinatari, generando involontariamente una comunicazione a catena dei dati personali raccolti. Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, e fare incorrere in sanzioni disciplinari, pecuniarie e in eventuali reati. (da vademecum privacy del Garante)

➤ L'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini, quando autorizzato dai docenti, è consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte (siano essi studenti o professori) in particolare della loro immagine e dignità.

Le istituzioni scolastiche hanno, comunque, la possibilità di regolare o di inibire l'utilizzo di registratori, smartphone, tablet e altri dispositivi elettronici all'interno delle aule o nelle scuole stesse. Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso. ( da vademecum privacy del Garante)

### **Registrazione delle lezioni e strumenti compensativi:**

➤ Nell'ambito dell'autonomia scolastica, gli istituti possono decidere di regolamentare diversamente o anche di inibire l'utilizzo di apparecchi in grado di registrare. In ogni caso deve essere sempre garantito il diritto degli studenti con diagnosi DSA (disturbi specifici dell'apprendimento) o altre specifiche patologie di utilizzare tutti gli strumenti compensativi (come il registratore) di volta in volta previsti nei piani didattici personalizzati che li riguardano. (da vademecum privacy del Garante)

➤ È consigliabile utilizzare canali istituzionali per comunicazioni a scopo didattico con le famiglie/tutor e gli studenti

➤ Come e-mail si utilizzerà quella istituzionale della scuola (nome.cognome@koinemonza.edu.it) per averne tracciabilità della conversazione in un

- luogo protetto.
- Le fotografie o i video da pubblicare sul sito che includano studentesse e studenti saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli.
  - I nomi completi di studentesse e studenti saranno evitati sul sito web come pure nei blog, forum e wiki, in particolare se in associazione con le loro fotografie.
  - All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video delle/dei minori secondo i principi sopra indicati.
  - Ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che varrà solo per lo specifico evento.

## **4. STRUMENTAZIONE PERSONALE durante l'orario scolastico**

(smartphone, tablet, pc portatili)

### **4.1 Per la componente studentesca.**

Nella scuola primaria si chiede alle famiglie di non lasciare i dispositivi ad alunne e alunni. Individui con disturbi specifici di apprendimento o altre disabilità certificate, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili.

Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

### **4.2 Per la componente personale scolastico docenti/ata**

I docenti possono utilizzare i dispositivi della scuola per realizzare tutte le attività connesse alla funzione docente. È consentito per i docenti l'uso dei propri dispositivi in classe per quanto attiene l'attività didattica qualora siano necessari, ma non possono essere utilizzati durante le lezioni per questioni personali.

Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, ...); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche programmate.

L'uso improprio della rete è contestato al titolare delle credenziali con cui è avvenuta la comunicazione.

### **4.3 Utilizzo del Laboratorio di Informatica e delle postazioni di lavoro**

Disposizioni sull'uso del laboratorio

1. Le apparecchiature presenti nella scuola sono patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione

- del personale docente e non docente.
3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando l'orario di ingresso, quello di uscita e motivazione dell'uso delle postazioni informatiche. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.
  4. L'ingresso delle studentesse e degli studenti nei laboratori è consentito solo in presenza dell'insegnante.
  5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
  6. Nei laboratori è vietato utilizzare CD personali o altri dispositivi se non dopo opportuno controllo con sistema di antivirus aggiornato.
  7. È vietato cancellare o alterare files-dati presenti sull'hard disk.
  8. Vietato alterare le impostazioni del PC, di rete o altro.
  9. Il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il mobilio in ordine, le macchine spente correttamente (chiudi sessione...).
  10. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.
  11. In caso di malfunzionamento non risolvibile dal responsabile di laboratorio si contatterà personalmente o attraverso il Responsabile di laboratorio, la segreteria.
  12. Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso. Si consiglia pertanto di salvare i dati importanti su Cd o penne usb periodicamente. In caso di formattazione ordinaria ci sarà un preavviso.
  13. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante.
  14. Il Responsabile di laboratorio che verifica un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

## **5 PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI**

### **5.1 Prevenzione**

La Scuola ha scelto una politica interna che sia pro-attiva, tesa cioè a creare un ambiente di apprendimento sereno e sicuro in cui sia chiaro sin dal primo giorno di scuola che (cyber)bullismo, prepotenza, aggressione e violenza non sono permessi, in cui ci sia l'apertura necessaria all'incoraggiamento a parlare di sé e dei propri problemi, che stimoli alla partecipazione diffusa di tutta la comunità scolastica nelle azioni finalizzate al contrasto del (cyber)bullismo, che insegni ad interagire in maniera responsabile.

#### **5.1.1 Rischi e Azioni della scuola rivolte agli studenti e alle loro famiglie/tutori.**

Il nostro istituto integra l'offerta formativa con attività finalizzate alla prevenzione e al contrasto del bullismo e del cyberbullismo, nell'ambito delle tematiche afferenti a Cittadinanza e Costituzione per tradurre i "saperi" in comportamenti consapevoli e corretti, indispensabili a consentire alle giovani generazioni di esercitare la democrazia nel rispetto della diversità e delle regole della convivenza civile. Le indicazioni relative ad un utilizzo sicuro della Rete da parte degli studenti potranno essere oggetto di specifici moduli didattici, da inserire nel Piano dell'Offerta Formativa (POF).

RISCHI	AZIONI
Adescamento online (grooming)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet, videogiochi, shopping o gambling online, ...	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.
Esposizione a contenuti pornografici, violenti, razzisti, ...	<i>Verso i genitori/tutori:</i> informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. <i>Verso la componente studentesca:</i> inserimento nel curriculum di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.
Sexting e pedopornografia.	<i>Verso i genitori/tutori:</i> informazione circa le possibilità di attivare forme di controllo parentale della navigazione. <i>Verso la componente studentesca:</i> inserimento nel curriculum di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con le studentesse e gli studenti e rispettivi genitori/tutori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.

Violazione della privacy	<p>Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare.</p> <p>Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione.</p> <p>Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative e/o penali.</p>
--------------------------	--

## 5.2 Sportello di ascolto

Tra le misure di prevenzione che la scuola mette in atto ci sono, altresì, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze così che l'utilizzo di Internet e dei cellulari oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di lucidità i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni. A tal proposito è attivo uno "Sportello di ascolto" rivolto a tutti gli studenti, articolato in colloqui individuali e/o collettivi, al fine di migliorare il benessere personale e scolastico mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale. Prevede, al suo interno, anche uno spazio riservato ai docenti e genitori al fine di individuare strategie efficaci per affrontare problematiche tipiche dell'età adolescenziale

## 5.3 Rilevazione

Compito dell'intera comunità educante è rilevare i casi, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. A partire dalla corretta formazione e sensibilizzazione, tutti gli adulti coinvolti, docenti e personale ATA sono invitati a essere confidenti e custodi, diretti o indiretti, di ciò che le ragazze e i ragazzi vivono: *si raccomanda di evitare ogni atteggiamento accusatorio o intimidatorio per riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute.*

Le/gli insegnanti in particolare sono chiamati a essere anche torre di avvistamento, spazio di avamposto privilegiato delle problematiche, dei rischi, dei pericoli che bambine, bambini e adolescenti possono vivere e affrontare ogni giorno. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni -quando non illegali- diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.

### 5.3.1 Come segnalare: procedure operative e strumenti

#### PROCEDURE OPERATIVE IN CASO DI SOSPETTO O EVIDENTE CASO DI CYBERBULLISMO:

1.	<b>Ascolta:</b> chiedigli/le cosa puoi fare per lui/lei e cosa desidera che accada;
2.	Se l'alunno ci porge spontaneamente le prove i docenti possono consultarle e dividerle con lui.
3.	<b>Avvisare e comunicare immediatamente l'accaduto al Dirigente scolastico,</b> al vicario e al referente cyberbullismo
4.	<b>Avere un colloquio con la "vittima" o accogliere la sua segnalazione</b> alla presenza di chi ha rilevato il caso, del referente del cyberbullismo e della dirigente scolastica (o vicario)
5.	Assicurarsi <b>che l'alunno vittima salvi nel suo telefono ogni messaggio,</b> voce/testo/immagine, conservando così il numero del mittente.

<b>6.</b>	<b>Avvisare telefonicamente i genitori/tutori</b> della vittima che conservi e condivida il contenuto e fare in modo che la famiglia si accerti della segnalazione ricevuta.
<b>7.</b>	<b>Conservare la prova, per il genitore/tutore, è utile</b> per far conoscere l'accaduto in base alla gravità ai genitori/tutori delle studentesse e degli studenti bulli, al Dirigente scolastico e per le condotte criminose alla polizia.
<b>8.</b>	Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori/tutori e per fatti rilevanti anche al Dirigente scolastico; per quelle criminose, anche alla polizia.
<b>9.</b>	<b>Accertarsi del danno</b> e avere copia o screenshot della conversazione dal genitore/tutore della vittima
<b>10</b>	<b>Intervenire con il protocollo di intervento (ALLEGATO 3):</b> agite per ridare benessere alla studentessa o studente.
<b>11</b>	<b>Avere un colloquio con il "bullo/bulli",</b> alla presenza di chi ha rilevato il caso, del referente del cybebullismo e del dirigente scolastico ( o vicario)
<b>12</b>	<b>Chiamare per un colloquio i genitori/tutori del "bullo o dei bulli",</b> per condividere la gravità della situazione rilevata e comunicare le successive azioni da mettere in atto
<b>13</b>	In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.
<b>14</b>	<b>fermare immediatamente l'abuso</b>
<b>15</b>	<b>Consultare il numero 1.96.96,</b> soprattutto nei casi gravi o complessi.
<b>16</b>	<b>Convocare il consiglio di classe</b> che nel caso sia necessario applichi eventuali sanzioni
<b>17</b>	<b>Applicare la sanzione</b> comunicandolo ai genitori/tutori.
<b>18</b>	<b>Avvisare in casi gravi la Polizia Postale e delle Comunicazioni</b>

- **Gli strumenti per segnalare e monitorare i casi a scuola**

Qui di seguito puoi trovare due strumenti che potranno agevolare LA SEGNALAZIONE.

1. nell'effettuare la segnalazione seguire ed utilizzare il **"modulo apposito di segnalazione" ALLEGATO 1** affinché le segnalazioni vengano effettuate per iscritto e contengano tutte le informazioni necessarie alla presa in carico della situazione.
2. Utilizzare poi **l'ALLEGATO 2 – "Diario di bordo "**per tenere traccia di ciò che è avvenuto rispetto ai comportamenti delle studentesse e studenti online e di come è stato gestito.

L'obiettivo a lungo termine è quello di creare una memoria condivisa non solo di ciò che accade nella scuola rispetto al web, ma anche di strutturare una fonte esemplificativa che possa orientare sempre più e sempre meglio le azioni di contrasto ad episodi che, nel tempo, potrebbero ripetersi

### **5.3.2 Come gestire le segnalazioni**

La gestione dei casi rilevati va differenziata a seconda della loro gravità;

- fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe.
- Altri casi ancora possono essere affrontati convocando genitori/tutori e studentesse e studenti per riflettere insieme su quanto accaduto e come rimediare.
- Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire

Inoltre, per *i reati meno gravi* la legge rimette ai genitori/tutori delle studentesse e degli studenti la scelta di richiedere la punizione del colpevole, attraverso la querela.

Per *i reati più gravi* (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).

In particolare, per i *fatti criminosi*, ai fini della denuncia, la relazione deve essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

In generale è bene tenere presente di:

- ✚ lavorare sul gruppo classe affinché riconosca la gravità dell'accaduto e la propria partecipazione attraverso il silenzio o forme blande di coinvolgimento;
- ✚ dare supporto al bullo con un programma educativo che si focalizzi su due fronti il coinvolgimento attivo del gruppo dei pari per sviluppare l'empatia e l'intervento dei docenti per gestire l'aggressività e la rabbia.

Come già detto per la prevenzione, il coinvolgimento dei coetanei è indispensabile per garantire l'efficacia dell'intervento ed è finalizzato a:

- ❖ creare un clima di solidarietà
- ❖ combattere l'indifferenza e la deresponsabilizzazione morale
- ❖ incoraggiare le vittime a chiedere aiuto
- ❖ sottrarre al (cyber)bullo potenziali proseliti

- **IL NUMERO 1.96.96. e servizi di ascolto o segnalazione**

La *linea di ascolto 1.96.96* (attiva 24 ore su 24, 365 giorni all'anno) e la *chat* (attiva tutti i giorni dalle 8.00 alle 22.00 (sabato e domenica dalle 8.00 alle 20.00) di **Telefono Azzurro** accolgono qualsiasi richiesta di ascolto e di aiuto da parte di bambini/e e ragazzi/e fino ai 18 anni o di adulti che intendono confrontarsi su situazioni di disagio/pericolo in cui si trova un minore. Il servizio di helpline è riservato, gratuito e sicuro, dedicato ai giovani o ai loro familiari che possono chattare, inviare e-mail o parlare al telefono con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza online.

Inoltre, è disponibile il **servizio Hotline** che 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 Center sono:

- **Clicca e segnala** di Telefono Azzurro [www.azzurro.it/it/clicca-e-segnala](http://www.azzurro.it/it/clicca-e-segnala)
- **Stop-it** di Save the Children [www.stop-it.it](http://www.stop-it.it)

Le segnalazioni relative alla presenza di materiale pedopornografico online sono inviate al Centro Nazionale per il Contrasto della Pedopornografia su Internet (C.N.C.P.O.), istituito presso il servizio di Polizia Postale e delle Comunicazioni, seguendo procedure concordate e nel rispetto della privacy del segnalante, come disposto dalla legge in materia.

**È importante fornire solo le informazioni che si hanno a disposizione e non attivarsi per ricercarne altre:** in questo caso si rientrerebbe nella ricerca proattiva di materiale pedopornografico e di conseguenza passibili di reato.

Avvisare in casi gravi la **Polizia Postale e delle Comunicazioni** è attualmente impegnata in diverse attività a sostegno della navigazione protetta dei minori ed è competente a ricevere segnalazioni su qualsiasi tipo di reato informatico.

- **Che succede quando segnali?**

Sulla base della segnalazione ricevuta, gli operatori di entrambi i Servizi (HOTLINE E TELEFONO AZZURRO) procedono a coinvolgere le Autorità competenti per la gestione degli interventi più opportuni a fronte del contenuto o della piattaforma segnalata. Seppur la condivisione della maggior quantità di dettagli e informazioni sul contenuto segnalato agevoli le successive indagini delle Autorità competenti, le Hotline analizzano e prendono in carico tutte le segnalazioni. È bene specificare però che, trattandosi di materiali spesso illegali, all'utente non è richiesto di cercare più informazioni rispetto a quelle che già possiede al momento della segnalazione. Nel caso di materiale pedopornografico, infatti, ciò potrebbe configurare attività passibili di reato come la ricerca proattiva di materiale pedopornografico. È quindi importante compilare con cura i campi richiesti dalle procedure guidate di segnalazione, riportando le informazioni rilevate accidentalmente, senza voler colmare eventuali mancanze; questo sarà il compito delle Autorità o dei Servizi che gestiranno nello specifico il caso. Le segnalazioni vengono trasmesse da entrambi i Servizi al C.N.C.P.O. ovvero il Centro Nazionale per il Contrasto della Pedopornografia Online, istituito presso il Servizio di Polizia Postale e delle Comunicazioni; tale organo valuterà se procedere ad approfondite indagini, a fronte delle quali mettere in atto opportuni interventi.

#### **5.4. Come gestire i casi**

Per questo la nostra Scuola opererà una politica di intervento sia **reattiva** che **pro-attiva**. Quella **reattiva** dovrà prevedere azioni di supporto al (cyber)bullo perché compia un processo di maturazione che lo porti a comprendere che qualsiasi forma di sopraffazione non è accettabile. Quella **proattiva**, richiede la partecipazione di tutte le componenti della comunità scolastica e dovrà essere rivolta a insegnare a tutti, potenziali bulli e vittime, sia come essere assertivi, sia come saper gestire la propria aggressività e istinto di sopraffazione, promuovendo un'interazione tra pari più responsabile.

Le procedure interne per la rilevazione e la gestione dei casi, nonché la segnalazione alla Dirigenza Scolastica ed eventualmente alle autorità competenti, avvengono secondo i protocolli suggeriti dalla piattaforma messa a disposizione da "Generazioni Connesse", come da schemi allegati.

##### **5.4.1 Procedura per gravi casi di cyberbullismo:**

In riferimento alla legge 1/2017 nel caso in cui un minore sia oggetto di **ATTI DI CYBERBULLISMO GRAVI, PESANTI e REITERATI NEL TEMPO**, è prevista la richiesta di oscuramento, rimozione o blocco di qualsiasi dato personale del minore medesimo.

La richiesta è effettuata dal minore che abbia compiuto i quattordici anni o (per i minori di 14 anni) dal genitore/tutore o dall' esercente la responsabilità genitoriale e va inoltrata:

- ☒ al titolare del trattamento
- ☒ al gestore del sito internet
- ☒ al gestore del social media

Se i soggetti responsabili non comunicano di aver preso in carico la segnalazione entro 24 ore dal ricevimento della stessa, l'interessato può rivolgersi, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali.

Il Garante provvede entro quarantotto ore dal ricevimento della richiesta.

Altre modalità di segnalazione riguardano quelle, effettuate dalle scuole, di episodi di cyberbullismo e materiale pedopornografico on line.

I primi (episodi di cyberbullismo) vanno segnalati al servizio Helpline di Telefono Azzurro

1.96.96, una piattaforma integrata che si avvale di telefono, chat, sms, whatsapp e skype. Tali strumenti, leggiamo nelle Linee di Orientamento, solo adeguati ad aiutare i ragazzi e le ragazze a comunicare il proprio disagio.

Quanto alla segnalazione di materiale pedopornografico, va effettuata alla Hotline "Stop-It" di Save the Children. Attraverso procedure concordate, le segnalazioni sono poi trasmesse al Centro Nazionale per il Contrasto alla pedopornografia su Internet, istituito presso la Polizia Postale e delle Comunicazioni.

#### ***5.4.2 Nuovi strumenti introdotti dalla L. 71/2017: l'ammonimento***

L'ammonimento è uno strumento di prevenzione, volto ad evitare il coinvolgimento del minore, sia quale autore del reato sia quale vittima, in procedimenti penali.

L'istanza di ammonimento nei confronti del minore ultraquattordicenne, autore di atti di cyberbullismo, va rivolta al Questore.

È possibile ricorrere all'ammonimento soltanto nel caso in cui non vi siano reati perseguibili d'ufficio o non sia stata formalizzata querela o presentata denuncia per le condotte di ingiuria (reato depenalizzato), diffamazione, minaccia o trattamento illecito dei dati personali, commessi mediante la rete Internet nei confronti di un altro minorenne.

La richiesta può essere presentata ad un qualsiasi ufficio di Polizia e deve contenere una dettagliata descrizione dei fatti, delle persone a qualunque titolo coinvolte ed eventuali allegati comprovanti quanto esposto.

Se l'istanza è ritenuta fondata, anche a seguito di approfondimenti investigativi, il Questore convoca il minore responsabile insieme ad almeno un genitore o ad altra persona esercente la potestà genitoriale; procede quindi ad ammonire oralmente il minore, invitandolo a tenere una condotta conforme alla legge con specifiche prescrizioni che varieranno in base ai casi.

Gli effetti dell'ammonimento cessano al compimento della maggiore età.

## 5.5 Azioni disciplinari di infrazioni accertate per uso scorretto dello smartphone

INFRAZIONE			SANZIONE DISCIPLINARE
FUORI ORARIO SCOLASTICO	tra compagni di classe	<b>Diffusione di foto o video non autorizzate</b> , tra compagni di classe fuori orario scolastico. È compreso il divieto alla condivisione su gruppi.	<p>- <b>richiamo scritto riportato sul Registro di classe</b> ;</p> <p>- <b>comunicazione formale alla famiglia</b>;</p> <p>- <b>comunicazione formale al Dirigente</b> dei ripetuti richiami scritti sul Registro ed alla famiglia.</p> <p>- <b>deferimento al Consiglio di Classe</b> /Interclasse (delle classi parallele del plesso coinvolto) quali organi collegiali preposti alle sanzioni sino a 15 giorni.</p>
		<b>Offese e insulti tramite messaggi</b> di testo, e-mail, pubblicati su social network (whatsapp, instagram, face book, etc...) tra compagni di classe fuori orario scolastico. Compresa anche la condivisione e diffusione	
		<b>Diffusione di foto o video</b> che ritraggono situazioni <b>intime, violente o spiacevoli</b> tramite il cellulare, siti web o social network, tra compagni di classe fuori orario scolastico, compresa la condivisione su gruppi.	
		<b>Furto, appropriazione, uso e rivelazione ad altri di informazioni personali</b> come le credenziali d'accesso all'account e-mail, social network, tra compagni di classe fuori orario scolastico	
	A personale scolastico	<b>Offese e insulti tramite messaggi di testo</b> , e-mail, pubblicati su social network (whatsapp, instagram, facebook, etc...) sul personale scolastico fuori orario scolastico. Compresa la sua diffusione e condivisione su gruppi.	
		<b>Diffusione di foto o video non autorizzate</b> in cui sia <b>presente personale scolastico</b> fuori dall'orario scolastico è compreso anche il <b>divieto alla condivisione su gruppi</b>	
INTERNO ALL' ORARIO SCOLASTICO	tra compagni di classe	<b>Offese e insulti tramite messaggi di testo</b> , e-mail, pubblicati su social network (whatsapp, instagram, facebook, etc...) a compagni all'interno dell'orario scolastico e nei locali della scuola, compreso la sua <b>condivisione e diffusione</b> su gruppi.	<p><b>POSSIBILI SANZIONI:</b></p> <p>- <b>richiamo scritto riportato sul Registro di classe</b>;</p> <p>-comunicazione formale alla famiglia;</p> <p>- comunicazione formale al Dirigente</p> <p>-<b>deferimento al Consiglio di Classe</b> /Interclasse quali organi collegiali preposti alle sanzioni asino a 15 giorni.</p> <p>-<b>Deferimento al consiglio d'Istituto</b> per violazioni disciplinari di estrema gravità: per ripetuti e gravi atti di bullismo o cyberbullismo accertati e avvenuti all'interno della scuola</p>
		<b>Diffusione di foto o video non autorizzate</b> a compagni all'interno dell'orario scolastico e nei locali della scuola. E' compreso anche il <b>divieto alla condivisione su gruppi</b> .	
	A personale scolastico	<b>Offese e insulti tramite messaggi di testo</b> , e-mail, pubblicati su social network (whatsapp, instagram, facebook, etc...) a <b>personale scolastico</b> all'interno dell'orario scolastico e nei locali della scuola. È compresa anche la <b>condivisione e diffusione</b>	
		<b>Diffusione di foto o video non autorizzate del personale scolastico</b> all'interno dell'orario scolastico e nei locali della scuola. È compreso anche il <b>divieto alla condivisione su gruppi</b> .	