Certificazione
ISO 9001-2000
n. 6849

Organismo di Formazione accreditato dalla Regione del Veneto

ISTITUTO PROFESSIONALE STATALE INDUSTRIA E ARTIGIANATO
"FEDELE LAMPERTICO"
Viale GG. Trissino, 30 – 36100 **VICENZA**
☎ 0444/504324 r.a.- C.F. 80014770244 – VIRI05000V@istruzione.it
www.lampertico.gov.it - VIRI05000V@pec.istruzione.it

POLICY DI E-SAFETY

Sommario

VISTA la Direttiva MIUR n. 16 del 5 febbraio 2007 recante " linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo";

VISTA la direttiva MPI n.30 del 15 marzo 2007 recante "linee di indirizzo ed indicazioni in materia di utilizzo d i" telefoni cellulari" e di altri dispositivi elettronici durante l' attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti";

VISTA la direttiva MPI n.104 del 30 novembre 2007 recante" linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all' utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali;

VISTA la direttiva MIUR n. 1455/06;

VISTO il D.P.R. 249/98 e 235/2007 recante "Statuto delle studentesse e degli studenti";

VISTE le linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyber bullismo, MIUR aprile 2015;

VISTA la Dichiarazione dei diritti in internet del 14 luglio 2015;

VISTA la Legge 29 maggio 2017 n. 71;

VISTI gli artt.3-33-34 Cost. italiana;

VISTI gli artt.581-582-594-595-610-612-635 del Codice penale;

VISTI gli artt.2043-2047-2048 Codice civile.

1. INTRODUZIONE

Scopo della Policy

La scuola, luogo principale di formazione, inclusione ed accoglienza, si impegna sul fronte della prevenzione del bullismo, e, più in generale di ogni forma di violenza e intende attivare strategie di intervento utili ad arginare comportamenti a rischio determinati , in molti casi, da condizioni di disagio sociale non ascrivibili solo al contesto educativo scolastico.

Pertanto il Nostro Istituto, stante il dilagare di queste nuove forme di devianza da parte degli adolescenti intende attivare sinergie con le famiglie e con le istituzioni, con l' obiettivo di accrescere il senso della legalità , il benessere e educare gli studenti ad un uso consapevole del web.

La rapida diffusione delle tecnologie, ha determinato, accanto al bullismo, un aumento del fenomeno del cyber bullismo, ossia quella forma di bullismo che viene esercitata attraverso un uso improprio dei social network, con la diffusione di foto, immagini denigratorie, tendenti a mettere a disagio, in imbarazzo o ad escludere. Si tratta di forme di aggressioni e molestie, spesso accompagnate dall' anonimato e dal fatto che la distanza del persecutore rispetto alla vittima rende più difficile la percezione della sua sofferenza. Il mondo digitale e virtuale, pur rappresentando un'enorme opportunità di sviluppo e crescita culturale e sociale, nasconde una serie di insidie e pericoli su cui è indispensabile misurarsi.

In tale ottica, si è ritenuto di avviare un percorso diretto a sostenere gli studenti e le famiglie sui temi della e Safety. Nell'ambito di tale percorso è stato elaborato, attraverso il coinvolgimento e la partecipazione attiva di docenti e genitori, il presente documento il quale è volto a definire:

- norme comportamentali e procedure per l'utilizzo delle Tecnologie della Società dell'Informazione (TSI) nell'ambito dell'Istituto;
- misure atte a facilitare e promuovere l'utilizzo positivo delle TSI nella didattica e negli ambienti scolastici;
- misure per la prevenzione e per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

La Scuola, nell' ambito dell' educazione alla legalità e all' uso consapevole di internet, si impegna a prevenire, individuare e combattere il bullismo e il cyberbullismo in tutte le loro forme .

2. Dettaglio degli scopi di questa policy:

- impostare i principi fondamentali che ci si aspetta e che verranno condivisi da tutti i membri della comunità scolastica rispetto all'uso delle TIC;
- salvaguardare e proteggere, i ragazzi e tutto il personale;
- assistere il personale della scuola per lavorare in modo sicuro e responsabile con Internet e altre tecnologie informatiche e di comunicazione;
- monitorare i propri standard e le prassi;
- Impostare chiare aspettative di comportamento per un uso accettabile e responsabile di Internet a scopo didattico. Tali comportamenti saranno da praticare anche a livello personale fuori dall'ambito scolastico;
- avere procedure chiare per affrontare un uso improprio degli strumenti digitali o gli abusi online come il cyberbullismo;
- assicurarsi che tutti i membri della Comunità scolastica sono consapevoli del fatto che i comportamenti illeciti o pericolosi sono inaccettabili e che verranno intraprese azioni appropriate, disciplinari e/o giudiziarie quando la situazione lo richiederà;

- ridurre al minimo il rischio di accuse fuori luogo o dannose fatte contro gli adulti che lavorano con gli studenti.

Le principali aree di rischio per la nostra Comunità Scolastica possono essere riassunte così:

3. Contenuti

- L'esposizione a contenuti dannosi e non appropriati (es. contenuti razzisti ecc.).
- Siti web che promuovono stili di vita e comportamenti dannosi (es. siti che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, ecc.).
- Contenuti che spingono all'odio.
- Validazione dei contenuti: come controllare l'autenticità e l'esattezza dei contenuti online.
- Pornografia.

4. Contatto

- Grooming (adescamento online), sfruttamento sessuale.
- Cyberbullismo e bullismo in tutte le forme.
- Il furto di identità, comprese le password.
- Pedopornografia (con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone minorenni).

5. Condotta

- I comportamenti aggressivi (cyberbullismo e bullismo).
- Violazione della privacy, tra cui la divulgazione di informazioni personali o di dati (foto, video, voce) senza autorizzazione dei soggetti interessati.
- Reputazione digitale.
- Salute e benessere: dipendenza da Internet e quantità di tempo speso online (Internet Addiction – i/le ragazzi/e che ne soffrono sono spesso inconsapevoli ma, lontani dalla Rete, manifestano presto insofferenza, irascibilità e altri sintomi di disagio), gioco d'azzardo o gambling, videogiochi online in comunità mondiali (alcuni rischi associati possono essere ad esempio: contatti impropri con adulti, contenuti violenti e/o inadeguati; acquisti incontrollati, ecc.), l'immagine del corpo.
- Sexting.
- Copyright (poca cura o considerazione per la proprietà intellettuale e i diritti d'autore).

6. Ruoli e Responsabilità

Ruolo	Responsabilità Chiave
Dirigente Scolastico	• Deve essere adeguatamente formato sulla sicurezza e prevenzione di problematiche offline e online, in linea con le leggi di riferimento e i suggerimenti del MIUR e delle sue agenzie. • Deve promuovere la cultura della sicurezza online integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto. • Ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, suoi strumenti ed ambienti. • Ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segue le pratiche migliori possibili nella gestione dei dati stessi.

	• Deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet. • Previsione ragionevole di adeguamento: entro prossimo triennio tutto l'Istituto con configurazioni diverse a secondo dell'utenza e dei bisogni formativi espressi. • Ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non. • Deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online. • Deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto. • Ricevere le relazioni di monitoraggio periodiche della sicurezza online dal Referente al termine di ciascun anno scolastico. • Garantisce che ci sia un sistema di monitoraggio della rete e personale di supporto che metta in atto procedure di sicurezza on-line interne in collaborazione con le successive figure di sistema. • Assicura che sito web della scuola includa informazioni sulla cultura della sicurezza online, rilevanti e condivise con i diversi stakeholders.
Referente della Sicurezza Online	• Il Referente e il team della sicurezza si fanno carico giorno per giorno della responsabilità dei problemi di sicurezza online e sono riferimento per la creazione e la revisione delle politiche di sicurezza online della scuola e dei relativi documenti. • Si impegnano a promuovere la cultura della sicurezza on-line in tutta la comunità scolastica. • Garantiscono che l'educazione all'uso consapevole delle TIC e alla sicurezza online sia inserita all'interno del curricolo di studi degli studenti. Il Referente e il team devono garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente di sicurezza on-line. • Collaborano, al bisogno e se è il caso, con il personale tecnico (anche esterno) in forza alla Scuola.

	• Il Referente comunica con il team e la componente genitori per discutere questioni, controllo di filtraggio per un aggiornamento adeguato.

Gli adulti hanno un ruolo fondamentale nel garantire che gli studenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro, ruolo che vede coinvolti a pieno titolo tutti coloro che hanno un ruolo educativo, oltre che formativo, primi fra tutti i genitori e la comunità scolastica nel suo complesso.

Non va tuttavia sottovalutato il ruolo degli studenti come primi attori del percorso di acquisizione della capacità di positiva gestione delle proprie competenze digitali: in tale ottica si rende indispensabile coinvolgere anche i più giovani, non solo quali destinatari, ma anche interlocutori attivi e propositivi di tutte le azioni e gli interventi volti alla piena attuazione della Policy.

7. Condivisione e comunicazione della Policy all'intera comunità scolastica

Il presente documento, frutto di un lavoro di condivisione e confronto con la partecipazione di docenti e famiglie, è reso oggetto di condivisione da parte dell'intera comunità scolastica sia in fase di elaborazione (attraverso il coinvolgimento delle famiglie), sia attraverso l'approvazione da parte degli Organi Collegiali.

Di esso viene data ampia diffusione a tutta la Comunità Scolastica, attraverso la pubblicazione sul sito web istituzionale.

8. Gestione delle infrazioni alla Policy

Tutte le infrazioni alla presente Policy andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere.

- La Scuola prenderà e manterrà nel tempo tutte le precauzioni necessarie e adatte per garantire agli studenti l'accesso a materiale e ambienti appropriati, anche se è impossibile evitare in assoluto che essi trovino materiale indesiderato navigando su un computer della scuola.

La scuola non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dall'accesso ad internet.

- Il Referente per il bullismo e il suo team sono coloro ai quali bisogna rivolgersi immediatamente nel caso in cui si verifichino incidenti o comportamenti dubbi.
- Qualsiasi sospetto, rischio, violazione va segnalato in giornata al suddetto Referente che riferisce al Dirigente.
- Al personale, agli studenti e agli altri componenti della comunità scolastica sono date informazioni sulle infrazioni previste e le eventuali sanzioni.
- Le sanzioni riferite soprattutto agli alunni avranno come carattere preferenziale quello educativo/riabilitativo e in ogni caso verrà coinvolta la componente genitori, in qualità di primi educatori.
- All'interno del Regolamento d'Istituto si trovano invece le diverse sanzioni, graduate in modo proporzionale rispetto alla gravità delle varie forme di bullismo (art. 4 DPR 249 del 1998).
- E' fondamentale per l'Istituto, anche nella sanzione, creare sempre occasioni di recupero. Risulta infatti possibile commutare i giorni di sospensione con attività socialmente utili alla comunità

scolastica o alle associazioni convenzionate.

9. Monitoraggio dell'implementazione della Policy e suo aggiornamento

La e-safety policy sarà riesaminata annualmente e/o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola.

Sarà rivista in relazione a norme di maggior valore come regolamenti o Policy emanati dal MIUR o eventuali leggi dello Stato.

10. Integrazione della Policy con Regolamenti esistenti

La e-safety policy fa riferimento e si armonizza con tutti gli altri regolamenti vigenti nell'Istituto in particolare con le Norme generali di comportamento con relativa tabella di sanzioni previste.

Va ad integrare tale regolamento costituendo la sezione relativa all'uso delle nuove tecnologie, dei nuovi ambienti di apprendimento e metodologie didattiche offerti dall'Istituto (es. Aule Smart-PON 2012/2020, didattica BYOD, GS4E learning enviroment/sistema di cloud computing).

Tutto ciò che qui non è normato è da considerarsi regolamentato secondo la disciplina generale.

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti:

- PTOF
- POF
- Regolamento interno
- Regolamento per l'utilizzo dei laboratori multimediali.

11. FORMAZIONE E CURRICOLO

Curricolo sulle competenze digitali per gli studenti

Con la raccomandazione 2006/962/CE del Parlamento Europeo e del Consiglio dell'Unione europea, viene individuato un quadro di riferimento europeo in materia di competenze chiave per l'apprendimento permanente. Tra queste viene individuata la competenza digitale, ovvero il "saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione."

Al fine di promuovere l'acquisizione delle competenze digitali, verranno svolte attività dirette a perseguire i seguenti obiettivi:

- conoscere e acquisire consapevolezza su natura, ruolo e opportunità delle TSI nel quotidiano;
- distinguere il reale dal virtuale, pur riconoscendone le correlazioni;
- sviluppare le abilità di base nelle TSI (uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni);

- usare le informazioni in modo critico, accertandone la pertinenza;
- acquisire consapevolezza su come le TSI possono coadiuvare la creatività e l'innovazione;
- riflettere sulle problematiche legate alla validità e all'affidabilità delle informazioni disponibili;
- acquisire consapevolezza sulle opportunità e sui potenziali rischi di Internet e della comunicazione tramite i supporti elettronici;
- riflettere sui principi giuridici ed etici di base che si pongono nell'uso interattivo delle TSI (netiquette, privacy…).

In virtù della valenza trasversale delle competenze digitali, la loro acquisizione viene promossa attraverso percorsi didattici disciplinari e/o interdisciplinari inerenti diverse aree, coerentemente con gli obiettivi individuati nel Curricolo di Istituto.

12. Formazione dei docenti

Al fine di favorire il continuo aggiornamento sui temi delle tecnologie digitali, sia in termini di utilizzo ed integrazione delle TSI (Tecnologie della Società dell'informazione) nella didattica, sia di utilizzo consapevole e sicuro di Internet e delle tecnologie digitali, verranno promosse iniziative volte al confronto ed allo scambio di idee e pratiche innovative:

- attività formative interne (seminari, workshop, attività laboratoriali), avvalendosi di risorse interne e/o esterne;
- diffusione di informazioni circa opportunità formative esterne in presenza e/o a distanza.

13. Sensibilizzazione delle famiglie.

In considerazione dell'importanza di favorire la sinergia degli interventi educativi di Scuola e famiglia per il successo scolastico ed educativo di ogni studente, il presente documento è allegato al Patto Educativo di Corresponsabilità stipulato con le famiglie degli alunni quale l'impegno reciproco di scuola e famiglia alla corresponsabilità formativa, nella quale rientrano a pieno titolo i temi legati alla eSafety.

Allo scopo di mantenere viva l'attenzione delle famiglie sui tali temi, verranno inoltre valorizzate le opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

14. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE DELLA SCUOLA

L'infrastruttura e la strumentazione dell'Istituto sono un patrimonio di tutti, esse vanno utilizzate nel rispetto delle norme contenute nel "Regolamento per l'utilizzo dei laboratori multimediali". I danni causati alle attrezzature saranno a carico di chiunque disattenda il suddetto Regolamento.

L'accesso ad infrastrutture e strumentazione utilizzabili per la didattica è riservato agli insegnanti e

agli alunni ed è limitato al perseguimento di scopi formativi. I docenti devono formare i propri alunni al rispetto del suddetto Regolamento, per gli aspetti di loro pertinenza.

15. STRUMENTAZIONE PERSONALE

a) Studenti

Non è consentito agli alunni della scuola di portare a scuola nessun tipo di device, fatta eccezione per le macchine fotografiche prive di connessione dati, che potranno essere utilizzate durante le uscite didattiche.

La Scuola sconsiglia agli alunni di portare il telefono mobile. Ciò è comunque consentito per motivi familiari e organizzativi. Coerentemente con quanto indicato dalla Direttiva Ministeriale n. 30 del 15 marzo 2007 e successive modificazioni, gli studenti sono però tenuti a tenere il telefono spento durante tutto il periodo di permanenza a scuola e in ogni ambiente. **I telefoni verranno conservati nello zaino o in apposito contenitore chiuso, individuato e gestito dai docenti, che verrà trasportato a cura del docente in servizio ove la classe si sposti all'interno della scuola per motivi didattici. In tal caso essi verranno depositati all'inizio delle lezioni e riconsegnati al termine delle medesime a cura del docente in servizio, così come è previsto anche dal regolamento d'Istituto.**

In caso di violazione delle suddette disposizioni, sarà previsto il ritiro temporaneo dei dispositivi da parte del docente che rileva la violazione. Quest'ultimo dovrà tempestivamente informare la famiglia dell'accaduto (anche telefonicamente), annotare la violazione sul registro elettronico e compilare in maniera molto meticolosa una "Scheda per la rilevazione di violazione delle disposizioni sulla strumentazione personale" (di seguito allegata) e disponibile nell'area riservata del sito web istituzionale. Il modulo andrà consegnato negli uffici di segreteria per essere protocollato. Alla seconda infrazione la famiglia verrà convocata dal Dirigente Scolastico per un colloquio. Il telefono ritirato verrà riconsegnato allo studente al termine delle lezioni.

Ai sensi della Direttiva Ministeriale n. 30 del 15 marzo 2007, con la condivisione della presente Policy, "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone" a seguito di violazioni della presente policy.

b) Docenti

I docenti sono autorizzati ad utilizzare devices personali in classe unicamente per fini didattici e professionali. In tal caso la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente al proprietario.

c) Personale della scuola

Tutto il personale scolastico è autorizzato ad utilizzare devices personali laddove non stia assolvendo ad un ruolo didattico, a condizione che l'utilizzo non intralci il normale svolgimento delle attività scolastiche, né distragga dal corretto svolgimento delle proprie mansioni. In tal caso la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente al proprietario.

Nell'invitare tutta la comunità scolastica (studenti, docenti, personale e famiglie) ad evitare, per quanto non necessario, la pubblicazione in rete di immagini e/o video ripresi all'interno dell'Istituto (fatta salva la pubblicazione da parte dei docenti in relazione a scopi didattici e/o

professionali, previa informativa al Dirigente Scolastico), è bene ricordare che, secondo la normativa vigente, non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese e che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere in gravi violazioni, incorrendo in sanzioni disciplinari, pecuniarie ed eventuali reati.

16. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Per i ragazzi nativi digitali le interconnessioni tra vita e tecnologia sono la normalità. Essi, pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti e tale fenomeno è tanto maggiore quanto è più forte il coinvolgimento emotivo nell'utilizzo dei nuovi media.

Ciò fa sì che alcuni rischi che fanno parte del mondo digitale possano non essere percepiti come tali ed è dunque compito degli adulti, famiglie ed insegnanti, affrontarli con l'obiettivo di prevenirli.

Tra i principali rischi, sia di carattere comportamentale che di matrice tecnica, ricordiamo:

- possibile esposizione a contenuti violenti e non adatti alla loro età;
- videogiochi diseducativi;
- pubblicità ingannevoli;
- accesso ad informazioni scorrette;
- virus informatici in grado di infettare computer e cellulari;
- possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e (adescamento);
- rischio di molestie o maltrattamenti da coetanei (bullismo e cyberbullismo);
- scambio di materiale a sfondo sessuale (sexting);
- uso eccessivo di Internet/cellulare (dipendenza).

L'I.P.S.I.A. Lampertico è da tempo impegnato nell'attivazione di iniziative volte a promuovere la cultura dell'inclusione, visto il largo numero di studenti provenienti da diverse nazioni, del rispetto dell'altro/a e delle differenze, nonché dell'utilizzo consapevole, positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TSI).

A tal fine è responsabilità di ciascun docente cogliere ogni opportunità per riflettere insieme agli alunni sui rischi in oggetto, nonché monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente, anche mediante il ricorso alle figure di sistema specializzate, per sostenere il singolo nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'instaurazione di un clima positivo, di reciproca accettazione e rispetto, nelle situazioni di difficoltà socio-relazionale.

Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i temi sopra menzionati, cui la Scuola porrà particolare attenzione, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

17. Rilevazione

Laddove il docente colga possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati nel paragrafo "Prevenzione", potrà chiedere il supporto del docente Referente per il bullismo e cyberbullismo, compilando la "scheda di segnalazione" (di seguito allegata e disponibile nell'area riservata del sito web istituzionale). La scheda di segnalazione potrà essere redatta dal docente sia sulla base di eventi osservati direttamente a scuola, sia su eventi particolari che gli sono stati confidati dall'alunno o comunicati da terzi.

18. Gestione dei casi

A seguito della segnalazione, il docente Referente insieme al suo team avrà cura di contattare il docente per un colloquio finalizzato a valutare la necessità di effettuare uno o più interventi di osservazione in classe e, successivamente, di pianificare adeguati interventi educativi e, ove necessario, di coinvolgere le famiglie per l'attivazione di un percorso comune e condiviso di sostegno al disagio.

Le azioni poste in essere dalla Scuola saranno dirette non solo a supportare le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, ma anche a

realizzare interventi educativi rispetto a quanti abbiano messo in atto comportamenti lesivi, ove si tratti di soggetti interni all'Istituto.

Nel casi di maggiore gravità si valuterà anche il coinvolgimento di attori esterni quali le forze dell'ordine e i servizi sociali.

19. Rilevazione e gestione

Che cosa segnalare	***Come segnalare: quali strumenti e a chi.***	***Come gestire le segnalazioni. Tempi di massima di presa in carico***
Navigazione in siti inadeguati. Documenti inadeguati lasciati su pc e/o condivisi. Acquisizione e/o uso di immagini, registrazioni video e audio, documenti in modo non congruo alla policy. Discussioni via mail, social o chat istantanee che influiscono in modo negativo sui comportamenti assunti o usate in modo difforme da questa policy (anche casi di abusi, cybrbulismo, bullismo ecc).	***In caso di minore:*** registrazione sul registro di classe (elettronico e con comunicazione alla famiglia). ***Per tutti:*** Di persona o via comunicazione telefonica: al Referente e contestualmente al D.S./vicario. In ogni caso il D.S. deve essere tempestivamente informato. In caso di situazione particolarmente grave verrà richiesta contestuale verbalizzazione scritta da	Ogni segnalazione verrà valutata da DS, dal Referente e dal suo team che attiveranno a seconda della gravità dei fatti e rispetto alle evidenze, sicuramente entro una settimana dal fatto, le procedure di sanzione (compreso quelle di competenza degli organi collegiali) e se necessario gli enti governativi competenti con relativo verbale di accompagnamento. Ogni segnalazione verrà valutata da DS e dal Referente e dal suo team che attiveranno a seconda della gravità dei fatti e rispetto alle evidenze ma sicuramente entro una settimana dal

	parte del dichiarante. ***Per tutti:*** Di persona o via comunicazione telefonica: al Coordinatore della sicurezza e contestualmente al D.S./vicario. In ogni caso il D.S. deve essere messo tempestivamente al corrente. Per i casi più gravi verrà richiesta contestuale verbalizzazione scritta da parte del dichiarante e se si tratta di minore ci sarà il coinvolgimento immediato dei genitori.	fatto, le procedure di sanzione accompagnamento (comprese quelle di competenza degli organi collegiali) e se necessario gli enti governativi competenti con relativo verbale di accompagnamento.

In ogni situazione di sofferenza o disagio legato anche al mondo delle TIC è possibile:

- riferire direttamente agli insegnanti o al referente per il bullismo e cyberbullismo e suoi collaboratori. Questi, dopo consultazione del Dirigente Scolastico, indirizzeranno l'alunno insieme alla famiglia verso i passi da compiere, rispetto alla gravità della situazione e se necessario metteranno in atto azioni di monitoraggio e accompagnamento.
- usufruire dello Sportello Ascolto attivo nel nostro Istituto. Esso è luogo di ascolto ***neutro*** e ***riservato***.

Lo psicologo se interpellato, valuterà secondo etica professionale, i singoli casi e come procedere. È invitato tuttavia a condividere con i referenti istituzionali nei limiti di rispetto del segreto professionale informazioni e azioni volte alla tutela e al benessere dei minori.

20. Procedure operative per la gestione delle infrazioni alla E-Safety Policy.

Ogni volta che un membro del personale o studente viola la E-Safety Policy, la decisione finale sul livello di sanzioni sarà a discrezione del Dirigente Scolastico e rifletterà le procedure comportamentali e disciplinari della Scuola.

Di seguito sono fornite solo come esemplificazione:

STUDENTI:

INFRAZIONI	***POSSIBILI SANZIONI***
• L'uso di siti non-educativi durante le lezioni. • L'utilizzo non autorizzato di e-mail. • L'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) durante le lezioni. • Uso di instant messaging / siti di social networking.	Fare riferimento all'insegnante della classe/ E-Safety Coordinator/Dirigente Scolastico

• L'uso continuato di siti non-educativi durante le lezioni dopo essere stato avvertito. • L'uso non autorizzato di e-mail dopo essere stato avvertito. • L'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) dopo essere stato avvertito. • L'uso continuato messaggistica / chat room istantanea, siti di social networking, newsgroup. • L'uso di materiale offensivo.	Fare riferimento all'insegnante della classe/ E-Safety Coordinator/Dirigente Scolastico Escalation a: • rimozione dei diritti di accesso a Internet per un periodo; • rimozione di telefono fino a fine giornata; • contatto con i genitori.
• Rovinare o distruggere deliberatamente i dati di qualcuno, violare la privacy altrui o messaggi inappropriati , video o immagini su un sito di social networking. • Invio di un messaggio e-mail o MSN che è considerato molestia o azione di bullismo. • Cercare di accedere a materiale offensivo o pornografico.	Fare riferimento all'insegnante della classe/ E-Safety Coordinator/Dirigente Scolastico Escalation a: **1.** rimozione dei diritti di accesso a Internet per un periodo; **2.** rimozione del telefono fino a fine giornata; **3.** contatto con i genitori; contattare le autorità competenti.
• Invio di e-mail o messaggi di MSN considerati molestia o bullismo dopo essere stato avvertito. • Accedere deliberatamente allo scaricamento o alla diffusione di qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento. • Trasmissione di materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati. • Portare il nome della scuola in discredito.	Fare riferimento all'insegnante della classe/ contatto con i genitori Altre possibili azioni di salvaguardia: **1.** conservare le prove; **2.** informare i provider di servizi di posta elettronica del mittente; **3.** fare rapporto alle autorità competenti dove si sospetti la pedofilia o altre attività illegali.

PERSONALE SCOLASTICO:

INFRAZIONI	**POSSIBILI SANZIONI**
• Uso di internet per attività personali non legate allo sviluppo professionale (shopping online, e-mail personali, instant messaging)	• Fare riferimento all' E-Safety Referente/DSGA /Dirigente Scolastico Escalation a: 1. Avvertimento

• Gravi danni intenzionali all'hardware o software del computer. • Qualsiasi tentativo deliberato di violare la protezione dei dati o di sicurezza informatica. • Creare, accedere, scaricare e diffondere deliberatamente qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento. • Ricevere o trasmettere materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati. • Portare il nome della scuola in discredito	Fare riferimento all'E-Safety Coordinator/ DSGA /Dirigente Scolastico Altre azioni di salvaguardia: **1.** rimuovere il PC in un luogo sicuro per garantire che non vi è alcun ulteriore accesso al PC o laptop; **2.** far verificare tutte le attrezzature per garantire che non vi è alcun rischio di alunni che accedono a materiali inappropriati nella scuola. Escalation a: Contattare e fare rapporto alle autorità competenti.

Agli studenti e al personale scolastico docente e non docente è fatto divieto di utilizzare in modo improprio gli strumenti della scuola(Reti, Pc,….). Pertanto verrà segnalato all'autorità giudiziaria ogni accesso abusivo al sistema informatico ai sensi e nei limiti dell'art. 615 ter c.p. (utilizzo non autorizzato di strumenti , appropriazione password, blocco lim, ecc.)

Come saranno informati il personale e gli studenti di queste procedure?

La E-Safety Policy sarà resa disponibile sul sito dell'Istituto a studenti, personale scolastico e genitori. I genitori firmeranno la E-Safety Policy quando il loro figlio inizierà la Scuola.

Agli studenti sarà insegnato un uso responsabile della rete in modo tale che possano sviluppare "comportamenti sicuri".

Informazioni su come segnalare azioni di bullismo o cyber bullismo saranno messe a disposizione dalla Scuola per gli alunni, il personale e i genitori.

1 bis. PROCEDURA OPERATIVA IN CASO DI VIOLAZIONE DELLE DISPOSIZIONI SULLA STRUMENTAZIONE PERSONALE

RILEVAZIONE INFRAZIONE DISPOSIZIONE SULL'USO DEI TELEFONI MOBILI.					
CHI	DOCENTE	DOCENTE	DOCENTE	DOCENTE	DIRIGENTE SCOLASTICO
COSA FA	Ritiro telefono e riconsegna allo studente al termine delle lezioni	Informare immediatamente la famiglia anche telefonicamente in caso di minore	Annotazione di quanto accaduto sul registro elettronico	Compilazione e consegna in segreteria della scheda per la rilevazione di violazione	Convocazione delle famiglie

Prima infrazione

Seconda infrazione

2 bis. PROCEDURA OPERATIVA DI RILEVAZIONE E GESTIONE DEI CASI

Conoscenza diretta o indiretta di situazioni a rischio							
CHI	Docente	Docente	Docente referente bullismo	Team della sicurezza	Dirigente Scolastico	DS/Team della sicurezza/ Docente referente bullismo	DS
Cosa fa	Compilazione scheda di segnalazione	Consegna della scheda di segnalazione al docente referente bullismo	Colloquio con i docenti ed eventuali osservazioni in classe	Interventi educativi in classe	Convocazione delle famiglie	Colloqui con le famiglie	Intervento soggetti esterni
RISCHI DI LIEVE ENTITÀ'							
RISCHI DI MODERATA ENTITÀ'							
RISCHI DI ELEVATA ENTITA'							

Documenti da compilare in caso di infrazione.

ISTITUTO PROFESSIONALE STATALE INDUSTRIA E ARTIGIANATO

"FEDELE LAMPERTICO"

Viale GG. Trissino, 30 – 36100 **VICENZA**

☎ 0444/504324 r.a.- C.F. 80014770244 – VIRI05000V@istruzione.it

www.lampertico.gov.it - VIRI05000V@pec.istruzione.it

PRIMA SEGNALAZIONE EPISODI BULLISMO E CYBERBULLISMO A SCUOLA

Nome e cognome di chi compila il modulo di segnalazione:

_____

DATA_____/_____/_____

1. La segnalazione del presunto caso di bullismo è stata fatta:
   - dalla VITTIMA_____ (Indicare il nome)
   - da un compagno della vittima _____ (Indicare il nome)
   - dalla madre/dal padre /dal tutore della vittima _____ (Indicare il nome)
   - Insegnante _____ (Indicare il nome)

2) Vittima/e
   Nome_____
   classe frequentata dalla vittima
   ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 sez._____

   Eventuali altre vittime
   Nome_____
   classe frequentata dalla vittima
   ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 sez._____

   Nome_____
   classe frequentata dalla vittima
   ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 sez._____

3) Bullo/i
   Nome_____
   classe frequentata del bullo
   ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 sez._____
   Nome_____
   classe frequentata del bullo
   ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 sez._____

Nome_____

classe frequentata del bullo

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 sez._____

4) Ordine di scuola

- Primaria
- ☐ Sec.1°grado
- ☐ Sec.2°grado indirizzo di studio_____

5) Gli episodi sono stati segnalati anche da altre persone?

- ☐ da un compagno della vittima _____
  (Indicare il nome)
- ☐ dalla madre/dal padre /dal tutore della vittima _____
  (Indicare il nome)
- Insegnante_____
  (Indicare il nome)

6) Grado di sofferenza della vittima

○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10

7) Tipologia dell'episodio

- ☐ Bullismo
- ☐ Cyberbullismo

8) Breve descrizione del problema presentato. dare esempi concreti degli episodi di prepotenza (dove e quando?)

_____

_____

_____

9) Quante volte si sono verificati gli episodi?

_____

_____

_____

ISTITUTO DI ISTRUZIONE SUPERIORE

- **ISTRUZIONE PROFESSIONALE e servici per_____- Servizi_____;**
- **ISTRUZIONE tecnica -_____.**

Via_____n. __- CAP_____CITTA'_____,
TEL._____,
SEDE STACCATA_____,
SITO_____.

AL QUESTORE DELLA PROVINCIA DI _____

ISTANZA DI AMMONIMENTO

Il/la sottoscritta/o_____,

Nata/o_____, il _____/____/_____, a_____,

Residente_____in_____tel._____e-mail_____non avendo ancora sporto querela per i fatti di seguito narrati,

C H I E D E

che la S.V. proceda alla completa identificazione ed all'ammonimento nei confronti del/della Sig./Sig.ra_____il/la quale, con le proprie reiterate condotte di

- ☐ pressioni
- ☐ aggressione
- ☐ molestia
- ☐ ricatto
- ☐ ingiuria
- ☐ denigrazione
- ☐ diffamazione
- ☐ furto d'identità *(es: qualcuno finge di essere me sui social network, hanno rubato le mie password e utilizzato il mio account sui social network, ecc.)*

- alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali *(es: qualcuno ha ottenuto e diffuso immagini, video o informazioni che mi riguardano senza che io volessi, ecc.)*
- qualcuno ha diffuso online dati e informazioni (video, foto, post, ecc.) per attaccare o ridicolizzare me, e/o la mia famiglia e/o il mio gruppo di amici,

qui allegate, in particolare, i comportamenti posti in essere, **realizzati per via telematica.**

Il/la sottoscritta/o, si riserva inoltre la facoltà di sporgere querela nei confronti del/della Sig./Sig.ra_____nei previsti termini di legge.

Luogo e data _____

La Richiedente

_____

Modello per segnalare episodi di bullismo sul web o sui social network e chiedere l'intervento del Garante per la protezione dei dati personali

Con questo modello si può richiedere al Garante per la protezione dei dati personali di disporre **il blocco/divieto della diffusione online di contenuti ritenuti atti di cyberbullismo** ai sensi dell'art. 2, comma 2, della legge 71/2017 e degli artt. 143 e 144 del d.lgs. 196/2003

INVIARE A
Garante per la protezione dei dati personali
indirizzo e-mail: cyberbullismo@gpdp.it

IMPORTANTE - La segnalazione può essere presentata direttamente da un chi ha un'età maggiore di 14 anni o da chi esercita la responsabilità genitoriale su un minore.

CHI EFFETTUA LA SEGNALAZIONE?

(Scegliere una delle due opzioni e compilare TUTTI i campi)

☐ Mi ritengo vittima di cyberbullismo e **SONO UN MINORE CHE HA COMPIUTO 14 ANNI**	Nome e cognome Luogo e data di nascita Residente a Via/piazza Telefono E-mail/PEC
☐ Ho responsabilità genitoriale su un minore che si ritiene vittima di cyberbullismo	Nome e cognome Luogo e data di nascita Residente a Via/piazza Telefono E-mail/PEC **Chi è il minore vittima di cyberbullismo?** Nome e cognome Luogo e data di nascita Residente a Via/piazza

IN COSA CONSISTE L'AZIONE DI CYBERBULLISMO DI CUI TI RTIENI VITTIMA?

(indicare una o più opzioni nella lista che segue)

- ☐ pressioni
- ☐ aggressione
- ☐ molestia
- ☐ ricatto
- ☐ ingiuria
- ☐ denigrazione
- ☐ diffamazione
- ☐ furto d'identità *(es: qualcuno finge di essere me sui social network, hanno rubato le mie password e utilizzato il mio account sui social network, ecc.)*
- ☐ alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali *(es: qualcuno ha ottenuto e diffuso immagini, video o informazioni che mi riguardano senza che io volessi, ecc.)*
- ☐ qualcuno ha diffuso online dati e informazioni (video, foto, post, ecc.) per attaccare o ridicolizzare me, e/o la mia famiglia e/o il mio gruppo di amici

QUALI SONO I CONTENUTI CHE VORRESTI FAR RIMUOVERE O OSCURARE SUL WEB O SU UN SOCIAL NETWORK? PERCHE' LI CONSIDERI ATTI DI CYBERBULISMO?

(Inserire una sintetica descrizione – **IMPORTANTE SPIEGARE DI COSA SI TRATTA**)

_____

_____

_____

_____

_____

DOVE SONO STATI DIFFUSI I CONTENUTI OFFENSIVI?

- ☐ sul sito internet [è *necessario indicare l'indirizzo del sito o meglio la URL specifica*]
  _____
- ☐ *su uno o più social network* [*specificare su quale/i social network e su quale/i profilo/i o pagina/e in particolare*] _____
- ☐ altro [*specificare*] _____

Se possibile, allegare all'e-mail immagini, video, *screenshot* e/o altri elementi informativi utili relativi all'atto di cyberbullismo e specificare qui sotto di cosa si tratta.

1) _____
2) _____
3) _____

HAI SEGNALATO AL TITOLARE DEL TRATTAMENTO O AL GESTORE DEL SITO WEB O DEL SOCIAL NETWORK CHE TI RITIENI VITTIMA DI CYBERBULLISMO RICHIEDENDO LA RIMOZIONE O L'OSCURAMENTO DEI CONTENUTI MOLESTI?

- ☐ Si, ma il titolare/gestore non ha provveduto entro i tempi previsti dalla Legge 71/20017 sul cyberbulllismo *[allego copia della richiesta inviata e altri documenti utili]*;
- ☐ No, perché non ho saputo/potuto identificare chi fosse il titolare/gestore

HAI PRESENTATO DENUNCIA/QUERELA PER I FATTI CHE HAI DESCRITTO?

- ☐ Si, presso_____;
- ☐ No

Luogo, data

Nome e cognome

Informativa ai sensi dell'art. 13 del Codice in materia di protezione dei dati personali

Il Garante per la protezione dei dati personali tratterà i dati personali trasmessi, con modalità elettroniche e su supporti cartacei, per lo svolgimento dei compiti istituzionali nell'ambito del contrasto del fenomeno del cyberbullismo. Il loro conferimento è obbligatorio ed in assenza degli stessi la segnalazione/reclamo potrebbe non poter essere istruita. I dati personali potrebbero formare oggetto di comunicazione ai soggetti coinvolti nella trattamento dei dati personali oggetto di segnalazione/reclamo (con particolare riferimento a gestori di siti internet e social media), all'Autorità giudiziaria o alle Forze di polizia ovvero ad altri soggetti cui debbano essere comunicati per dare adempimento ad obblighi di legge. Ciascun interessato ha diritto di accedere ai dati personali a sé riferiti e di esercitare gli altri diritti previsti dall'art. 7 del Codice.

Questa e-safety policy con i suoi apparati è stata formulata in collaborazione con rappresentanti dei docenti, del personale tecnico e del Dirigente Scolastico.

Essa andrà ad integrare il Regolamento di Istituto - Norme Generali di Comportamento per la parte di competenza.

Vicenza 17 Maggio 2018

in fede Prof. Dirigente Scolastico: Aldo Delpari

La firma autografa è omessa ai sensi dell'art. 3, c.2, D.Lgs. 39/1993

Il docente Referente della proposta e stesura della e-policy

Prof. Mario Fiore