VIIC82800V - REGISTRO PROTOCOLLO - 0008261 - 22/11/2021 - E4 - U

ISTITUTO COMPRENSIVO VALDAGNO 1
Via Pasubio 171 – 36078 Valdagno (VI) - Tel. 0445-410428 – Fax 0445-426014
Indirizzi mail: viic82800v@istruzione.it; – P.E.C.: viic82800v@pec.istruzione.it
Sito web: www.icvaldagno1.edu.it

Documento di ePolicy

e

P.U.A

aggiornati per l'anno scolastico 2021-2022

Dirigente Scolastico dott.ssa Maria Catena LUPO

Documento a cura della *Commissione Bullismo* d'Istituto

con il supporto del *Safer Internet Centre* - Ministero dell'Istruzione

Firmato digitalmente da MARIA CATENA PALMINA OLIVIA LUPO

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse. Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico; le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento - Indice

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica 5. Gestione delle infrazioni alla ePolicy
    6. Integrazione dell'ePolicy con regolamenti esistenti
    7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica 3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità

3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**

1. Protezione dei dati personali
2. Accesso ad Internet
3. Strumenti di comunicazione online
4. Strumentazione personale

4. **Rischi on line: conoscere, prevenire e rilevare**

1. Sensibilizzazione e prevenzione
2. Cyberbullismo: che cos'è e come prevenirlo
3. Hate speech: che cos'è e come prevenirlo
4. Dipendenza da Internet e gioco online
5. Sexting
6. Adescamento online
7. Pedopornografia

5. **Segnalazione e gestione dei casi**

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio per intervenire
4. Allegati con le procedure

Perché è importante dotarsi di una e-Policy?

Attraverso l'e-Policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

L' e-Policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

Le principali aree di rischio per la nostra comunità scolastica riguardano i seguenti ambiti:

- **contenuto**: esposizione a contenuti e siti web non adeguati e non in linea con le finalità educative di Istituto, problemi legati all'autenticità e all'esattezza dei contenuti online;
- **contatto**: *grooming* (adescamento), cyberbullismo in tutte le sue forme, furto di identità;
- **condotta**: violazione della privacy (ad es. divulgazione di informazioni personali), reputazione online, diritti e doveri degli internauti (elementi fondamentali di Cittadinanza Digitale), netiquette, salute e benessere (quantità di tempo speso online su Internet o giochi), *sexting* (invio e ricezione di immagini personali intime), il rispetto del *Copyright*.

1.2 - Ruoli e responsabilità

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

Ruoli e Responsabilità (di tutti gli attori della Comunità Scolastica)

RUOLO	RESPONSABILITA'
Il Dirigente Scolastico	• garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica; • promuove la cultura della sicurezza online e corsi di formazione specifici, d'accordo con il docente Referente per il bullismo e il Cyberbullismo; • promuove la formazione di tutto il personale scolastico sull'uso positivo e responsabile delle tic, sulle potenzialità e i rischi della rete; • dà attuazione al protocollo di e-Policy e ne promuove l'aggiornamento; • fa parte del Team per l'Emergenza (insieme all'Animatore digitale, al Referente bullismo, allo psicologo individuato dall'Istituto) e del Team antibullismo (le forze dell'ordine, i servizi sanitari e la tutela dei minori, le strutture e le agenzie educative del territorio) per gestire e intervenire nei casi di gravi episodi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali; • intrattiene i rapporti con le agenzie competenti e le autorità locali; • promuove il coordinamento tra le figure istituzionalmente preposte all'utilizzo delle TIC a scuola (Responsabile della Sicurezza, Amministratore di sistema e Animatore Digitale).
Il Referente bullismo e cyberbullismo	• coordina le iniziative di prevenzione e di contrasto del bullismo e del cyberbullismo all'interno dell'Istituto; • fa parte del Team per l'Emergenza (insieme al Dirigente Scolastico, all'Animatore digitale, allo psicologo individuato dall'Istituto) e del Team antibullismo (le forze dell'ordine, i servizi sanitari e la tutela dei minori, le strutture e le agenzie educative del territorio) per gestire e intervenire nei casi di gravi episodi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali; • coordina la Commissione Bullismo della scuola (che ha un rappresentante per ogni plesso e ordine di scuola dell'Istituto Comprensivo), con il compito di proporre attività didattiche e iniziative volte a stimolare comportamenti responsabili, a sensibilizzare e a prevenire prevaricazioni e ogni forma di bullismo; • può avvalersi delle forze dell'ordine e delle associazioni del territorio; • coinvolge studenti, colleghi e genitori in progetti e percorsi formativi specifici;
L'Animatore digitale e il suo team	• supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai temi della sicurezza online; • può monitorare e rilevare le problematiche relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola; • promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo del PNSD; • può fare in modo che gli utenti autorizzati accedano alla Rete della scuola con apposita password e che i pc delle aule siano dotati di password; • fa parte del Team per l'Emergenza (insieme al Dirigente Scolastico, all'Animatore digitale, allo psicologo individuato dall'Istituto) e del Team antibullismo (le forze dell'ordine, i servizi sanitari e la tutela dei minori, le strutture e le agenzie educative del territorio) per gestire e intervenire nei

	casi di gravi episodi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali;
I docenti	• educano gli alunni ad un uso responsabile della rete e delle TIC; • promuovono l'uso delle tecnologie digitali nella didattica, accompagnando gli alunni nelle attività di apprendimento e nei laboratori che prevedono l'uso di dispositivi tecnologici; • informano gli alunni sulle procedure da seguire per la segnalazione di atti di bullismo e cyberbullismo; • si formano e autoformano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet; • hanno il dovere professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso che coinvolga gli studenti; • usano comportamenti sicuri, responsabili e professionali nell'uso della tecnologia;
Il personale Amministrativo,Tecnico e Ausiliario (ATA)	• usano comportamenti sicuri, responsabili e professionali nell'uso della tecnologia; • sono consapevoli dei problemi di sicurezza online connessi con l'uso di dispositivi multimediali; • hanno il dovere di segnalare qualsiasi sospetto abuso informatico alle figure di sistema, nonché di raccogliere verificare e valutare informazioni inerenti possibili casi di bullismo/cyberbullismo; • possono formarsi e auto-formarsi in tema di bullismo e cyberbullismo.
Gli studenti e le studentesse	• in relazione al grado di maturità e consapevolezza raggiunti, utilizzano le tecnologie digitali in coerenza con quanto richiesto dai docenti; • conoscono le linee guida dell'E-safety Policy, il Regolamento d'Istituto (relativamente all'uso non corretto dei dispositivi tecnologici e in materia di bullismo/cyberbullismo) e il Patto di Corresponsabilità, che hanno sottoscritto; • capiscono l'importanza di segnalare ad adulti di riferimento eventuali abusi o l'uso improprio della Rete e dei dispositivi digitali; • imparano a tutelarsi online, a tutelare compagni/e e a rispettarli/e • utilizzano i dispositivi tecnologici personali esclusivamente su autorizzazione del docente e solo per specifiche attività didattiche; • possono farsi promotori delle buone pratiche apprese, anche attraverso possibili percorsi di peer education.
I genitori	• sono partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete; • accettano e condividono l'e-Policy d'Istituto, il Regolamento d'Istituto e il Patto di Corresponsabilità; • conoscono le linee di intervento della Scuola in relazione ai problemi rilevati ad un uso non responsabile o pericoloso delle tecnologie digitali o di internet; • si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano TIC e la Rete, monitorando i propri figli e segnalando eventuali problemi .

1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio dell'interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

Gli enti educativi, gli specialisti, i formatori e le associazioni esterne che entrano in relazione con la scuola sono tenuti a conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC, adottando e promuovendo comportamenti sicuri e proteggendo gli studenti durante le attività che si svolgono assieme.

In coerenza con il percorso intrapreso dal nostro Istituto viene predisposta un'informativa sintetica sull'e-Policy comprensiva delle "procedure di segnalazione" in caso di illecito e di episodi che mettano in pericolo studenti e studentesse.

Le procedure di segnalazione devono contenere i riferimenti interni alla scuola cui rivolgersi in caso di necessità, come il Referente bullismo e il coordinatore della/e classe/i coinvolta/e nel progetto.

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

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

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

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

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione

semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

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

E' in progetto una versione *child friendly* del documento di e-Policy per la comunicazione e la sensibilizzazione ai bambini e alle bambine. Nella comunicazione e condivisione di questo documento è infatti importante valutare i vari target di riferimento, adeguando di conseguenza i linguaggi, le modalità e i canali comunicativi.

1.5 - Gestione delle infrazioni alla e-Policy

La scuola gestirà le infrazioni all'e-Policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni. Le sanzioni alternative, qualora se ne ravvisi l'utilità e l'opportunità, sono proposte dal Dirigente Scolastico e adottate dal Consiglio di Classe. Possono essere di tipo risarcitorio e riparatorio a favore della comunità scolastica e/o svolgimento di attività rieducative presso enti, associazioni.

Il nostro Istituto ritiene importante che le sanzioni possano trasformarsi anche in occasione di recupero e di crescita. Accanto ad esse, infatti, è opportuno stimolare comportamenti, volti al perseguimento di una finalità educativa. Risulta perciò possibile commutare il provvedimento di sospensione con attività socialmente utili alla comunità scolastica o ad associazioni convenzionate, quali attività di studio e ricerca a favore della classe e/o della comunità scolastica, preparazione di materiale da utilizzare nell'ambito di attività didattiche, riordino della biblioteca scolastica e/o di materiali utilizzati nelle lezioni di scienze motorie, arte o musica o altre attività suggerite dai componenti il Consiglio di classe, dallo studente interessato dal provvedimento e/o i suoi genitori per i minorenni.

Sulla base dell'e-Policy d'Istituto, dello Statuto delle studentesse e degli studenti e del Regolamento d'Istituto, gli studenti protagonisti di atti di bullismo verranno coinvolti in un percorso di comprensione della gravità degli atti compiuti e, se possibile, a mettere in atto comportamenti attivi riparatori (es. attività di volontariato, pulizia degli spazi scolastici, piccole manutenzioni, svolgimento di attività di assistenza o di volontariato nell'ambito della comunità scolastica o delle associazioni del territorio convenzionate).

Il nostro Istituto vieta l'uso di qualsiasi dispositivo digitale personale durante l'orario scolastico, tranne nel caso in cui venga proposta un'attività didattica da parte dell'insegnante, in sua presenza e sotto la sua supervisione. Diversamente, è fatto divieto assoluto agli alunni di utilizzare qualsiasi dispositivo digitale in classe, nei corridoi, nei bagni e in qualsiasi altro locale della scuola, compreso il cortile, durante la ricreazione. Il cellulare dovrà essere tenuto spento e riposto dentro lo zaino dal momento dell'ingresso fino alla fine delle lezioni.

<u>Disciplina degli alunni</u>

Gli ammonimenti della scuola sono proporzionati alle circostanze, secondo la seguente gradualità (ad eccezione dei casi più gravi):

- richiamo verbale;

- richiamo scritto con annotazione sul libretto personale e sul registro elettronico;

- convocazione dei genitori da parte degli insegnanti;
- convocazione dei genitori da parte del Dirigente Scolastico;
- eventuale provvedimento disciplinare e allontanamento (da 1 a 15 giorni) dell'alunno dalle attività didattiche.

Contestualmente sono messi in atto interventi di carattere educativo, quali la ridefinizione delle regole sociali della convivenza comune, la promozione di rapporti amicali e della solidarietà, il riconoscimento e la gestione delle emozioni (empatia), attività e lavori socialmente utili. Ove invece il fatto costituisca reato, si provvede alla segnalazione alle autorità competenti (Polizia, Carabinieri, Garante della Privacy).

Disciplina del personale scolastico

Il Dirigente Scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet. Eventuali infrazioni verranno trattate secondo le disposizioni previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori

E' importante che i genitori segnalino alla scuola eventuali episodi di cyberbullismo di cui venissero a conoscenza ed avvenuti in contesto scolastico. Essi sono responsabili di materiali inadatti al contesto scolastico introdotti a scuola dai propri figli. I genitori si assumono la responsabilità circa la divulgazione, la condivisione e un uso non consentito dalla legge di qualsiasi materiale (fotografie, video, registrazioni e/o materiali personali) relativo agli alunni o da questi detenuto.

Tabella della gestione delle infrazioni all'e-Policy con annesse sanzioni disciplinari. La tabella è desunta dal Regolamento d'Istituto, recentemente aggiornato.

MANCANZA DISCIPLINARE	SANZIONE/PROVVEDIMENTO	ORGANO COMPETENTE E PROCEDURA
Pronuncia di insulti, offese verbali, linguaggio blasfemo, espressioni maleducate e arroganti, mancanze di rispetto a compagni, docenti e personale della scuola.	● Richiamo verbale (a seconda della gravità è possibile adottare direttamente il secondo provvedimento) ● Nota sul libretto e relativa comunicazione scritta alla famiglia (con verifica della presa visione nel corso della lezione successiva) ● Alla terza violazione richiamo da parte del Dirigente scolastico e nota sul registro di classe. ● In caso di recidive, possibile provvedimento di sospensione dalle attività scolastiche da 1 a 3 giorni.	Docente dell'ora interessata e il Dirigente Scolastico. Se necessario, il Dirigente scolastico convocherà il Consiglio di Classe per discutere l'adozione della sanzione della sospensione.
Esercizio di qualsiasi forma di violenza fisica e/o	Richiamo del coordinatore di classe, comunicazione scritta (e telefonica, qualora se ne ravveda la necessità) alle famiglie degli	Il docente che verificherà la trasgressione procederà alla verbalizzazione

VIIC82800V - REGISTRO PROTOCOLLO - 0008261 - 22/11/2021 - E4 - U

atti di bullismo	alunni coinvolti. In caso di Bullismo eventuale coinvolgimento del Referente Bullismo e del Dirigente scolastico. A seconda della gravità è possibile adottare direttamente il secondo provvedimento. ● Nel caso di violenze fisiche senza gravi conseguenze, provvedimento di sospensione dalle attività scolastiche da 1 a 3 giorni ● Nel caso di violenze fisiche con gravi conseguenze e accertati atti di bullismo: allontanamento dalla comunità scolastica superiore da 3 a 15 giorni.	dell'infrazione. In caso di presunto bullismo, viene coinvolto il Referente Bullismo della scuola che, d'accordo con il Dirigente scolastico, porterà il caso in Team per l'Emergenza. Nei casi più gravi il Dirigente scolastico, rilevata la mancanza disciplinare, convocherà il Consiglio di Classe per la contestazione di addebito.
Uso di telefoni cellulari e altri dispositivi elettronici	**NON viene tollerato il rifiuto dell'allievo alla consegna immediata del dispositivo elettronico. Nel caso il docente non ottenesse la consegna, l'allievo verrà accompagnato dal Dirigente.**	Il docente che verificherà la trasgressione procederà alla verbalizzazione dell'infrazione. Nei casi più gravi il docente segnalerà al Dirigente scolastico la mancanza disciplinare, il quale convocherà il Consiglio di Classe per la contestazione di addebito.
L'alunno tiene il cellulare spento in vista sul banco oppure l'alunno ha il cellulare acceso.	● Richiamo verbale (1v.) ● Annotazione sul registro di classe con comunicazione alla famiglia sul libretto personale. (2.v) ● In caso di recidiva, l'alunno è tenuto a consegnare il dispositivo al docente che lo porterà in segreteria (3 v.), dove verrà contattata la famiglia (il dispositivo viene consegnato all'allievo dopo tre gg. dal ritiro o immediatamente ad un genitore). Comunicazione della trasgressione al Dirigente	Il docente che verificherà la trasgressione procederà alla verbalizzazione dell'infrazione. Nei casi più gravi il docente segnalerà al Dirigente scolastico la mancanza disciplinare, il quale convocherà il Consiglio di Classe per la contestazione di addebito.
L'alunno utilizza il cellulare a scuola per chiamate e/o messaggistica o altri usi non consentiti (giochi, ascolto musica, ecc.)	● ritiro immediato del dispositivo e consegna in Segreteria (il cellulare viene consegnato all'allievo dopo tre gg. dal ritiro o immediatamente ad un genitore), nota sul registro di classe e comunicazione telefonica alla famiglia (1v.). ● In caso di recidiva, provvedimento di	Il docente che verificherà la trasgressione procederà alla verbalizzazione dell'infrazione. Nei casi più gravi il docente segnalerà al Dirigente scolastico la mancanza disciplinare, il quale

Firmato digitalmente da MARIA CATENA PALMINA OLIVIA LUPO

VIIC82800V - REGISTRO PROTOCOLLO - 0008261 - 22/11/2021 - E4 - U

	sospensione dell'alunno da 1 a 3 giorni.	convocherà il Consiglio di Classe per la contestazione di addebito.
L'alunno fa foto e/o video in classe o negli ambienti della scuola, anche riprendendo se stesso o i compagni.	● ritiro immediato del dispositivo e consegna in Segreteria (il cellulare viene consegnato all'allievo dopo tre gg. dal ritiro o immediatamente ad un genitore). Intervento del Dirigente e convocazione della famiglia. ● In caso di recidiva, provvedimento di sospensione da 1 a 3 giorni.	In caso di episodio di Cyberbullismo o di violazione della privacy, il coordinatore di Classe informerà il Referente bullismo di Istituto o un membro della Commissione Bullismo (in caso la trasgressione si verifichi in uno dei plessi non della sede centrale) che poi riferirà al Dirigente Scolastico. Può rendersi necessario denunciare la trasgressione al Garante della Privacy.
L'alunno diffonde anche in rete e nei social network immagini/video/audio non autorizzati effettuati a scuola.	● Provvedimento di sospensione dell'alunno da 1 a tre giorni. ● In caso di recidiva, provvedimento di sospensione da 3 a 15 giorni.	In caso di episodio di Cyberbullismo o di violazione della privacy, il coordinatore di Classe informerà il Referente bullismo di Istituto o un membro della Commissione Bullismo (in caso la trasgressione si verifichi in uno dei plessi non della sede centrale) che poi riferirà al Dirigente Scolastico. Può rendersi necessario denunciare la trasgressione al Garante della Privacy.
Uso non consentito e scorretto della navigazione in rete a scuola da parte dello studente, condivisione di materiale inappropriato, accesso a internet dai laboratori di informatica della scuola, dalla LIM di classe e durante la Didattica Digitale Integrata.	● Nota sul libretto e relativa comunicazione scritta alla famiglia (con verifica della presa visione nel corso della lezione successiva) ● Nota sul registro di classe, seguita da convocazione della famiglia ● In caso di recidiva, richiamo del Dirigente.	Docente dell'ora interessata e il Dirigente scolastico

Firmato digitalmente da MARIA CATENA PALMINA OLIVIA LUPO

VIIC82800V - REGISTRO PROTOCOLLO - 0008261 - 22/11/2021 - E4 - U

INFRAZIONI COLLETTIVE **Furti, danneggiamenti, atti di violenza di cui non è possibile individuare i responsabili, ma che coinvolgono l'intera o la maggioranza della classe**	● Nota sul registro di classe seguita da comunicazione scritta alle famiglie (con verifica della presa visione nel corso della lezione successiva), unita alla riparazione personale del danno ● Provvedimento di sospensione dalle attività scolastiche da 1 a 5 giorni e risarcimento collettivo dei danni ● Annullamento di tutte le uscite didattiche, dei viaggi di istruzione e delle attività extracurriculari per gli studenti coinvolti /la classe.	Docente dell'ora interessata che informerà il Coordinatore di classe per la comunicazione alle famiglie, con le quali concorderà le modalità per la riparazione del danno. Il coordinatore di classe segnalerà al Dirigente scolastico la mancanza disciplinare e questi convocherà il Consiglio di classe per discutere la contestazione di addebito ed eventualmente provvedere all'annullamento delle visite e dei viaggi d'istruzione.

1.6 - Integrazione dell'e-Policy con Regolamenti esistenti

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

Il Regolamento d'Istituto è stato aggiornato con specifici riferimenti all'e-Policy, in coerenza con le LInee Guida Miur e le indicazioni normative generali.

L' e-Policy integra inoltre il Regolamento d'Istituto con l'inserimento della seguente norma:

"Utilizzo del laboratorio di Informatica, delle postazioni di lavoro e dell'utilizzo di Internet."

Disposizioni sull'uso del laboratorio d'informatica

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

2. Il laboratorio può essere utilizzato esclusivamente per attività di insegnamento e di formazione.

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

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

5. Nel laboratorio è consentito utilizzare dispositivi personali (cd, dvd, chiavette usb) solo su autorizzazione del docente e previa scansione antivirus del dispositivo.

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

7. All'uscita dal laboratorio, è compito di chi ne ha usufruito lasciare l'aula in ordine e spegnere correttamente i dispositivi informatici utilizzati.

8. In caso di malfunzionamento o guasto dei computer l'insegnante deve darne tempestiva segnalazione al

Firmato digitalmente da MARIA CATENA PALMINA OLIVIA LUPO

Responsabile del Laboratorio.

9. L'accesso al laboratorio è regolato da un registro cartaceo.

10. Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso.

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

Disposizioni sull'uso dei software nelle postazioni pc d'Istituto

1. I software installati sono ad esclusivo uso didattico.

2. In base alle leggi che regolano la distribuzione delle licenze, i software presenti in laboratorio non sono disponibili per il prestito individuale.

3. Solo l'amministratore di sistema è autorizzato all'installazione di nuovi software.

Accesso a Internet

1. L'accesso a Internet è consentito alle classi esclusivamente sotto la supervisione del docente.

2. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet. In caso di responsabilità da parte di un minore, ne risponde la famiglia.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il nostro piano d'azione

Azioni da svolgere entro un'annualità scolastica:

Organizzare dei momenti di presentazione del progetto Generazioni Connesse rivolto rispettivamente agli studenti, ai docenti, ai genitori.

Azioni da svolgere nei prossimi 3 anni:

Organizzare un evento di presentazione, consultazione e conoscenza dell'ePolicy rivolto rispettivamente agli studenti, ai docenti e ai genitori.

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più “intuitivo” ed “agile” rispetto agli adulti, ma non per questo sono dotati di maggiori “competenze digitali”.

Infatti, “la competenza digitale presuppone l’interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l’alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l’alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l’essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico” (“Raccomandazione del Consiglio europeo relativa alla competenze chiave per l’apprendimento permanente”, C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

Il Curricolo sulle competenze digitali della scuola del Primo Ciclo di Istruzione è trasversale alle discipline previste dalle Indicazioni Nazionali: la competenza digitale è ritenuta dall’Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d’oggi.

Avere competenza digitale significa padroneggiare le nuove tecnologie, ma soprattutto usarle con “autonomia e responsabilità” nel rispetto degli altri.

Le raccomandazioni Europee ci ricordano la *dimensione integrata degli aspetti tecnologici, cognitivi ed etici che coesistono nelle competenze digitali*:

- dimensione tecnologica: le tecnologie digitali sono indubbiamente strumenti per la risoluzione di molteplici problemi della vita quotidiana, ma possiedono una "grammatica" che occorre gradualmente imparare a conoscere;

- dimensione cognitiva: essa fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità;

- dimensione etica e sociale: fa riferimento sia alla capacità di gestire in modo sicuro i dati personali e altrui che alle abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

Nell’ambito del PNSD (paragrafo 4.2. sulle "Competenze e contenuti") l’Istituto si propone un programma di progressiva educazione alla sicurezza online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti, tra cui:

- progettare attività e laboratori di Coding;
- sviluppare strategie per insegnare a valutare e verificare le informazioni per accettarne l'esattezza;
- capire la necessità di mettere in atto un comportamento corretto anche quando si utilizza un ambiente

online;

- sapere che le identità online possono essere false e ingannevoli;
- comprendere che le informazioni personali pubblicate online sono vulnerabili; conoscere le principali regole che tutelano la privacy delle persone; con particolare attenzione al web, conoscere le principali regole del copyright;
- comprendere l'impatto di bullismo online, sexting, grooming e sapere come cercare aiuto in caso di pericolo;
- sapere come segnalare eventuali abusi on-line e come chiedere aiuto agli adulti.

Il **DigComp 2.1**, nello specifico ne "Il quadro di riferimento per le competenze digitali dei cittadini" si elencano ben otto livelli di padronanza per ciascuna delle seguenti aree della cittadinanza digitale:

1. Alfabetizzazione e dati: ovvero la capacità di cercare, selezionare e valutare le informazioni in Rete;

2. Comunicazione e collaborazione: saper riconoscere le giuste e appropriate modalità per comunicare e relazionarsi online;

3. Creazione di contenuti digitali: valutare le modalità più appropriate per modificare, migliorare e integrare contenuti e informazioni, creandone di nuovi e originali;

4. Sicurezza: imparare a proteggere i dati personali e i contenuti digitali, comprendendo i rischi e le minacce presenti negli ambienti digitali.

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

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

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

Tra i principali vantaggi legati all'utilizzo delle TIC nella didattica vi sono l'incremento della motivazione e del coinvolgimento attivo da parte degli alunni, la facilitazione dei lavori di gruppo e del confronto fra pari, l'arricchimento della proposta didattica e supporto all'apprendimento per gli studenti con Bisogni Educativi Speciali.

Il nostro Istituto intende implementare e incoraggiare la formazione personale dei docenti con corsi sull'uso delle TIC in ambito territoriale (ad esempio con iniziative promosse dall'Amministrazione e dalle scuole polo), ma anche interni alla scuola stessa, avvalendosi delle risorse di docenti esperti. Supporta anche l'auto aggiornamento dei singoli docenti.

Eventuale materiale didattico dei docenti può essere messo in rete, anche su siti personali collegati all'Istituto, sempre nell'ambito del presente regolamento e nel rispetto delle leggi.

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

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

Formare i docenti sulle tematiche in oggetto vuol dire non pensare esclusivamente all'alfabetizzazione ai media, ma anche considerare la sfera emotiva e affettiva degli studenti e delle studentesse che usano le nuove tecnologie. Questi ultimi infatti comunicano, esprimono se stessi e sviluppano l'identità personale e sociale anche attraverso i dispositivi tecnologici che sempre di più consentono loro di poter entrare in contatto con il mondo che li circonda.

Prestare attenzione a questi aspetti significa dare ai docenti gli strumenti per poter educare ragazzi ei ragazze alle emozioni in contesto onlife, modulando e gestendo i propri e altrui comportamenti, favorendo e promuovendo forme di convivenza civile.

L'Istituto intende prevedere, nel corso del triennio, specifici momenti di formazione personale e collettiva per i docenti, unitamente a momenti formativi di approfondimento (laboratori, eventi, giornate, ecc...) con le famiglie e gli studenti, per sensibilizzare l'intera comunità educante.

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

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'e-Policy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto. L'Istituto quindi si impegna:

- alla diffusione delle informazioni e delle procedure contenute nel documento di ePolicy;
- ad offrire incontri e conferenze con esperti interni ed esterni;
- a fornire sul sito www.icvaldagno1.gov.it un link per essere costantemente informati su progetti, attività e iniziative di sensibilizzazione e prevenzione al bullismo/cyberbullismo.

Il nostro piano d'azione

AZIONI (da sviluppare nell'arco del corrente anno scolastico 2021-2022)

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali/ sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

Sono "dati personali" le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona e che possono fornire molteplici informazioni sul suo conto (dai dati anagrafici a quelli "sensibili", di natura religiosa, etnica... fino a quelli giudiziari). Il "trattamento" di questi dati sono l'insieme di operazioni, digitalizzate e non, applicate ad essi e l'istituzione scolastica può trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali o quelli previsti dalla norma di settore. Un esempio di violazione della protezione dei dati personali è il trattamento di questi senza aver fornito all'interessato un'adeguata informativa in merito, o senza aver ricevuti uno specifico consenso.

Il nostro Istituto possiede tre modelli: due standard per il trattamento dei dati personali di studenti/genitori(modello A) e per il personale; infine c'è la liberatoria per l'autorizzazione all'uso della piattaforma di Google Spacework da parte degli studenti (modello B).

A) MODELLO DI LIBERATORIA per la protezione dei dati personali degli alunni e dei loro genitori o tutori

INFORMATIVA PRIVACY AI SENSI DEL REGOLAMENTO UE 2016/679 PER IL TRATTAMENTO DEI DATI DEGLI ALUNNI E DEI LORO GENITORI O TUTORI

Titolare del trattamento

Il Titolare del trattamento dei dati è l'ISTITUTO COMPRENSIVO 1 VALDAGNO, (telefono 0445410428 – email viic82800v@istruzione.it), nella persona del Dirigente Scolastico, legale rappresentante dell'Istituto, Dott.ssa Maria Catena Lupo (controllare dati di contatto).

Responsabili del trattamento

L'elenco dei responsabili esterni del trattamento dei dati personali, costantemente aggiornato, è disponibile presso il titolare su esplicita e motivata richiesta.

Responsabile Protezione dei Dati

Dott. Federico Croso - Telefono: 0163 03 50 22 - Email: dpo@gdprscuola.it

Finalità

I dati personali forniti alla presente Istituzione scolastica, anche se raccolti presso il Ministero dell'Istruzione e le sue articolazioni periferiche, saranno trattati dal personale della scuola soltanto nell'ambito delle finalità istituzionali, che sono quelle relative all'istruzione ed alla formazione degli alunni e quelle amministrative ad esse strumentali. Il trattamento dei dati sarà improntato ai principi di correttezza, liceità, trasparenza, limitazione delle finalità, esattezza, limitazione della conservazione, integrità e tutela della riservatezza e dei diritti individuali.

I dati personali definiti come "dati sensibili" o come "dati giudiziari" dal D. Lgs 30 giugno 2003 n. 196 e successive modifiche (Codice della Privacy) e i dati previsti dagli art. 9 e 10 del Regolamento Ue 2016/679, saranno trattati esclusivamente dal personale della scuola, appositamente incaricato, secondo quanto previsto dalle disposizioni di Legge e di Regolamento nel rispetto del principio di stretta indispensabilità dei trattamenti.

Conservazione e trattamento

I dati saranno conservati presso gli archivi del Titolare per tutta la durata del rapporto tra la famiglia e l'istituzione scolastica, per l'espletamento di tutti gli adempimenti di legge e per un tempo non superiore agli scopi per i quali sono stati raccolti. I dati saranno altresì comunicati esclusivamente ai soggetti competenti per l'espletamento di servizi necessari ad una corretta gestione del rapporto scolastico, con garanzia di tutela dei diritti dell'interessato. Sono autorizzati al trattamento dei dati: il personale amministrativo, tecnico e ausiliario in servizio presso l'Istituto; i docenti in servizio presso l'Istituto; eventuali docenti ed esperti esterni incaricati dalla scuola di svolgere attività di ampliamento dell'offerta formativa, come previsto dal PTOF. Il personale incaricato ha accesso ai dati a seconda delle mansioni e si attiene alle norme impartite e alle disposizioni di legge. E' vietato all'incaricato qualsiasi forma di diffusione e comunicazione di dati personali che non sia funzionale allo svolgimento dei compiti affidati ed è adeguatamente istruito sulle norme privacy previste dal Regolamento Ue 2016/679.

Il trattamento sarà effettuato sia con strumenti cartacei che elettronici, nel rispetto delle misure di sicurezza minime, così come previsto dal Regolamento Europeo, ad opera di soggetti appositamente incaricati.

Legittimazione e consenso

Nel corso del rapporto con la presente Istituzione scolastica, i dati personali verranno trattati dal personale della scuola nell'ambito delle finalità istituzionali, così come definite dalla normativa vigente: R.D. n. 653/1925, D.Lgs n. 297/1994, D.P.R. n. 275/1999; D.I. n. 44/2001 e le norme in materia di contabilità generale dello Stato; L. n. 104/1992, L. n. 53/2003, D.Lgs n. 165/2001, D.Lgs 196/2003, D.M 305/2006; D.Lgs 76/05; D.Lgs 77/05; D.Lgs 226/05; D.Lgs n. 151/2001; D.P.C.M. n. 185/2006; D.P.R. n. 89/2009; L. 170/2010; D.M. n. 5669/2011; D.P.R. 80/2013, D. Lgs 33/2013, D.L. 104/2013, convertito, con modificazioni, dalla L. 128/2013, L. 107/2015, D. Lgs 50/2016 e relativi decreti applicativi e tutta la normativa collegata alle citate disposizioni.

Si fa presente che il conferimento dei dati richiesti e il conseguente trattamento sono obbligatori, in quanto previsti dalla normativa sopra citata; l'eventuale rifiuto a fornire tali dati potrebbe comportare il mancato perfezionamento dell'iscrizione e l'impossibilità di fornire all'alunno tutti i servizi necessari per garantire il suo diritto all'istruzione ed alla formazione. Dovrà essere invece ottenuto dalla presente Istituzione scolastica il consenso dell'interessato per raccogliere e trattare i dati relativamente ai trattamenti complementari alle finalità istituzionali.

Destinatari

I dati personali potranno essere comunicati a soggetti pubblici (quali, ad esempio, ASL, Comune, Provincia, Ufficio scolastico regionale, Ambiti Territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) nei limiti di quanto previsto dalle vigenti disposizioni di Legge e di Regolamento e degli obblighi conseguenti per codesta Istituzione scolastica; i dati relativi agli esiti scolastici degli alunni potranno essere pubblicati mediante affissione all'albo della scuola secondo le vigenti disposizioni in materia. I dati da forniti potranno essere comunicati altresì alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente alla carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio. Potranno infine venire a conoscenza dei dati personali terzi soggetti che forniscono, a questa Istituzione scolastica, servizi strumentali (alle finalità di cui sopra), ferma restando la garanzia di tutela dei diritti dell'interessato. Tali soggetti agiranno in qualità di Responsabili o Incaricati del trattamento. La realizzazione di questi trattamenti costituisce una condizione necessaria affinché l'interessato possa usufruire dei relativi servizi.

Ai sensi dell'art. 96 del Codice della Privacy, ferma restando la tutela della riservatezza dell'alunno, al fine di agevolare l'orientamento, la formazione e l'inserimento professionale dell'alunno, i dati relativi agli esiti scolastici, intermedi e finali, e altri dati personali diversi da quelli sensibili o giudiziari, potranno essere comunicati o diffusi, anche a privati e per via telematica. La comunicazione avverrà esclusivamente a seguito di sua richiesta e i dati saranno poi trattati esclusivamente per le predette finalità.

I dati sensibili e giudiziari non saranno oggetto di diffusione; tuttavia, alcuni di essi potranno essere comunicati ad altri soggetti pubblici nella misura strettamente indispensabile per svolgere attività istituzionali previste dalle vigenti disposizioni di legge in materia sanitaria, previdenziale, tributaria, giudiziaria e di istruzione. I dati non verranno trasferiti a destinatari residenti in paesi terzi rispetto all'Unione Europea né ad organizzazioni internazionali, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Diritti

Al Titolare del trattamento o al Responsabile l'interessato potrà rivolgersi senza particolari formalità, per far valere i propri diritti, così come previsto dal Regolamento Europeo 2016/679; ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

L'interessato ha i seguenti diritti: di accesso; di rettifica; di cancellazione (diritto all'oblio); di limitazione del trattamento; di revoca del consenso, nei casi previsti dal Regolamento. L'interessato ha inoltre diritto alla portabilità dei dati e di proporre reclamo all'Autorità di controllo dello Stato di residenza (Garante Privacy).

Informazioni aggiuntive

Per consentire ai genitori l'assolvimento dell'obbligo di garantire l'istruzione dei figli maggiorenni, che siano ancora non autosufficienti e conviventi, così come indicato dalle norme vigenti e dai pronunciamenti giurisprudenziali, è permesso ai genitori medesimi l'accesso alle informazioni riguardanti il rendimento scolastico e la frequenza dei figli maggiorenni rientranti nelle categorie sopra indicate (non autosufficienti e ancora conviventi).

……, lì……..

IL DIRIGENTE SCOLASTICO Dott.ssa Maria Catena Lupo

B) MODELLO DI LIBERATORIA per l'uso di Google Workspace

(Ai genitori degli alunni nuovi iscritti di IC VALDAGNO 1)

OGGETTO: Consenso all'uso delle piattaforme digitali "Google WORKSPACE" – MODULO DA RESTITUIRE

L'Istituto Valdagno 1 vuole dare la possibilità agli studenti di tutto l'Istituto di usufruire delle risorse a scopo didattico messe a disposizione, in maniera gratuita, dalle piattaforme "Google Workspace" (email, Classroom, Meet...). Questi sistemi consentono di creare "classi virtuali" tramite le quali i docenti possono interagire con gli studenti sia in classe, durante l'orario scolastico, che da casa, in orario extrascolastico. Questa opzione potrà essere utilizzata da tutti i docenti delle classi, a loro discrezione, per comunicare coi rispettivi studenti.

Classroom è un ambiente digitale pensato e creato per l'uso ESCLUSIVAMENTE scolastico. E' organizzato in gruppi-classe o altri gruppi di lavoro creati dagli insegnanti e chiusi a persone o interferenze esterne. Gli studenti non possono comunicare privatamente fra di loro. Non c'è alcun tipo di pubblicità. Tale piattaforma offre la possibilità ai genitori, che vogliano farlo, di accedere ai dati riguardanti il/la proprio/a figlio/a, per essere a conoscenza delle attività svolte nelle classi virtuali e di come i ragazzi interagiscono con gli insegnanti. Gli studenti avranno un account di posta elettronica personale (un indirizzo email) con estensione @icvaldagno1.edu.it, nel rispetto dei regolamenti vigenti.

L'ANIMATORE DIGITALE

Prof. Campagnuolo Nicola

IL DIRIGENTE SCOLASTICO

Dott.ssa Maria Catena Lupo

Firmato digitalmente da MARIA CATENA PALMINA OLIVIA LUPO

I sottoscritti genitori ____ _____ _____ dell'alunno/a

_____ della classe_____ del plesso di _____

dichiarano di aver preso visione delle informative privacy e dei termini di servizio per l'utilizzo della piattaforma Google Workspace. Inoltre

1. ___ non autorizzano ____ autorizzano il proprio figlio ad iscriversi ad esse

2. ___ dichiarano di aver preso visione dell'"INFORMATIVA EX ARTT.13 E 14 DEL REGOLAMENTO UE 2016/679, PER IL TRATTAMENTO DEI DATI PERSONALI AI FINI DELL'ISCRIZIONE ED UTILIZZO DELLA PIATTAFORMA WORKSPACE riportata al punto 2) e conseguentemente e con riferimento alle seguenti finalità ivi indicate

____prestano

_____non prestano il consenso al trattamento dei dati del proprio figlio/a autorizzando la scuola all'iscrizione al servizio Google Workspace e alla creazione di un account nominativo dello studente, (casella mail con estensione @icvaldagno1.edu.it) per l'accesso dei servizi offerti dalla piattaforma Google Workspace.

Con la sottoscrizione della presente dichiariamo inoltre di:

- essere a conoscenza che tale account serve esclusivamente per lo svolgimento delle attività didattiche e per nessun motivo può essere ceduto a terzi e non deve essere utilizzato per archiviare comunicazioni e/o documenti personali;

- essere a conoscenza che l'Istituto declina ogni responsabilità per l'eventuale perdita o diffusione accidentale di informazioni personali e/o per un uso dell'account diverso da quello didattico;

- essere a conoscenza che GOOGLE WORKSPACE è conforme alle norme FERPA e l'impegno in tal senso è sancito nei contratti.

3. L'adesione di Google agli accordi Safe Harbor tra l'Unione Europea e gli Stati Uniti contribuisce ad assicurare che gli standard di protezione dei dati sono conformi a quanto stabilito dall'Unione Europea per le istituzioni scolastiche. Abbiamo letto le informative sull'adozione dei servizi di Google sulla sicurezza dei dati e la privacy come riportate e descritte nella relativa *Informativa* fornita dall'IC VALDAGNO 1.

Firma*_____ *_____

Nel caso firmi un solo genitore, egli dichiara di essere consapevole di esprimere anche la volontà dell'altro genitore che esercita la responsabilità genitoriale - consapevole delle conseguenze amministrative e penali, per chi rilasci dichiarazioni non corrispondenti a verità a i sensi del DPR 445/2000, dichiara di aver effettuato la scelta in osservanza delle disposizioni sulla responsabilità genitoriale di cui agli articoli 316, 337 ter e 337 quater del codice civile, che richiedono il consenso di entrambi i genitori.

3.2 - Accesso ad Internet

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

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

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

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

La Rete internet della scuola è gestita dal Comune di Valdagno e suddivisa tra i vari plessi.

Antivirus e firewall sono collocati a monte della consegna dei dati, attraverso filtri della Pasubio Tecnologie, che è l'ente appaltante del servizio.

L'infrastruttura tecnologica dell'Istituto IC Valdagno 1 è in parte cablata e in parte funzionante tramite wi-fi.

La scuola dispone in tutte le sue sedi di una rete internet, cui accedono i computer delle aule e dei laboratori (rete didattica) separatamente da quelli dell'amministrazione (rete segreteria). Per quanto concerne la rete amministrativa, lo storage è garantito da backup automatico su altra postazione. L'ottenimento delle credenziali per l'utilizzo della rete wifi è riservato ai docenti e al personale dell'Istituto. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.

L'Istituto può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni dispositivo tramite la verifica della cronologia di navigazione. E' vietato installare e scaricare da Internet software non autorizzati dall'amministrazione. L'utilizzo di unità di archiviazione e chiavette usb è autorizzata, previa opportuna scansione antivirus, per evitare qualsiasi tipo di infezione alla rete d'Istituto. Sui dispositivi della scuola non è garantito alcun servizio di backup.

Non è previsto l'accesso al wi-fi della scuola per gli studenti, che possono utilizzare la rete esclusivamente in presenza dei docenti, attraverso gli strumenti informatici in dotazione nella scuola.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Il nostro istituto utilizza strumenti di comunicazione sia interni (come il registro elettronico, l'email, applicativi e piattaforme di lavoro condiviso come Classroom) che esterni (il sito della scuola, durante la DDI la web-radio, il profilo dell'istituto sul social network Facebook). Ecco gli strumenti e i canali di comunicazione online dell'Istituto:

- email. L'account di posta elettronica della scuola è quello istituzionale, **viic82800v@istruzione.it**, utilizzato dagli uffici amministrativi.

- Google Workspace (con i suoi applicativi Classroom e Meet) per l'attività didattica e nei periodi di attivazione della Didattica Digitale Integrata.

- sito istituzionale: **icvaldagno1.edu.it**. La gestione del sito della scuola, la realizzazione, la progettazione e la rispondenza alle normative sono attualmente a cura della segreteria e di Nuvola-Madisoft. La scuola detiene i diritti d'autore (tramite protocollo informatico) dei documenti che si trovano sul proprio sito.

- profilo sul social network Facebook: **Istituto Comprensivo Statale Valdagno 1**

- Nuvola Madisoft : il registro elettronico che permette di gestire la comunicazione con le famiglie.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ***e-Policy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti

del Miur per l'uso dei dispositivi mobili a scuola (**BYOD, "Bring your own device"**).

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

La scuola fornisce un indirizzo di posta elettronica personale (nome.cognome@icvaldagno1.edu.it) a tutti gli studenti, le studentesse e a tutto il personale docente, attivo per il tempo di permanenza nell'istituto (la scadenza degli accessi è programmata al 31 agosto dell'anno di fine percorso scolastico). Studenti e docenti possono utilizzarlo per accedere alla piattaforma e-learning e a tutte le attività proposte dalla scuola, nonché permette di mettere in contatto più facilmente studenti e docenti.

La scuola non consente l'utilizzo del cellulare personale degli alunni all'interno dell'Istituto e in orario scolastico, se non su esplicita autorizzazione del docente e per determinate attività didattiche, previo accordo con studenti/esse e genitori; la scuola deve chiedere ai genitori dei minori di 16 anni di età il consenso all'uso di Internet a scuola per il loro figlio e per la pubblicazione dei suoi lavori e delle sue fotografie. Si ricorda che in Italia, con il recepimento del GDPR, l'età minima per l'accesso ai social network è di 14 anni, 13 con il consenso genitoriale (relativamente ai social statunitensi)

Il presente documento di Epolicy sanziona eventuali usi illeciti dei dispositivi digitali e l'Istituto è dotato di una P.U.A. (Politica d'Uso Accettabile delle tecnologie a scuola) sull'uso delle TIC.

Per i docenti e per il personale della scuola è consentito l'uso dello smartphone e di altri dispositivi elettronici personali durante le ore di lezione solo a scopo didattico ed integrativo di quelli scolastici disponibili.

La nostra scuola ha in progetto di dotarsi di una *netiquette* (ovvero tutte quelle regole di comportamento che devono essere osservate dagli utenti di Internet), da pensare, realizzare e condividere con studenti e genitori dell'Istituto.

Il nostro piano d'azione

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.

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

Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

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

4.1 - Sensibilizzazione e Prevenzione

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

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

- osservare altri commettere queste azioni.

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

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

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

Considerate le molteplici problematiche sociali che si manifestano in rete e che interessano o coinvolgono direttamente e indirettamente la scuola (bullismo, cyberbullismo, grooming, sexting, pedopornografia, le violazioni della Privacy, il furto di identità, il gioco d'azzardo online, le pressioni psicologiche di varia natura, sextortion, abusi e violenze,…), è fondamentale agire sia sulla sensibilizzazione dell'intera comunità scolastica che sulla prevenzione dei comportamenti a rischio.

Gli effetti benefici dell'attività di sensibilizzazione sono molteplici, perché ad esempio accrescono la consapevolezza del gruppo circa un determinato tema, incoraggiano il cambiamento di comportamento facilitando il coinvolgimento delle persone e diffondono consapevolezza tra l'opinione pubblica. Infatti è necessario impegnarsi, perché avvenga un cambiamento, a qualsiasi livello.

La **prevenzione** si classifica in tre livelli d'azione: la prevenzione universale, che riguarda tutti gli studenti potenzialmente a rischio; quella selettiva, dedicata ad uno gruppo specifico di studenti in cui la condizione di rischio è presente e infine quella indicata, ovvero l'intervento mirato sulle persone coinvolte (sia chi esprime comportamenti problematici che la vittima).

Firmato digitalmente da MARIA CATENA PALMINA OLIVIA LUPO

Ovviamente la prevenzione universale è quella che - tra tutte - chiama direttamente in campo l'azione congiunta di scuola, famiglia, associazioni sportive e società civile, collaborando in un progetto comune, ciascuno secondo la propria funzione formativa ed educativa.

E' inoltre importante che la scuola sia messa quanto prima al corrente di eventuali criticità, e che attraverso colloqui, apposite schede di osservazione o relazioni ad hoc, mantenendo un contatto diretto con le famiglie, l'ULSS e le autorità competenti (Polizia Postale, Carabinieri, Garante della Privacy dell'Infanzia, la Procura), possa contribuire ad agire tempestivamente per risolvere eventuali criticità.

Purtroppo, quando l'azione preventiva risulta tardiva o non efficace, occorre passare direttamente al contrasto dei fenomeni sopracitati, con altre modalità che verranno illustrate in seguito.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

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

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti; Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;

Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.

Nomina del Referente per le iniziative di prevenzione e contrasto che:

- Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
- Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Rispetto al bullismo, il cyberbullismo (o bullismo online) è una forma di prepotenza virtuale messa in atto attraverso l'uso di internet e delle tecnologie digitali. L'azione bullizzante non ha bisogno di essere ripetuta tante volte, perché

la natura della Rete è quella di essere "ovunque" e "per sempre".

Il Cyberbullismo è caratterizzato dal generare un impatto incontrollabile, attraverso la diffusione di materiale in Rete, di cui non è possibile prevedere limiti e confini. L'assenza di confini spaziali fa sì che il cyberbullismo possa avvenire ovunque; spegnere il cellulare non basta, come neppure cancellare i propri profili social.

Chi offende spesso è convinto di non essere identificabile. Purtroppo, quando ci si sente protetti dall'anonimato ci si sente più liberi e forti nel compiere atti denigratori, senza il timore di essere scoperti. Il cyberbullo non vede in modo diretto le reazioni della vittima, riducendo il riconoscimento del danno provocato. L'anonimato è un falso mito della Rete, perché ogni nostra azione è rintracciabile, con strumenti opportuni o con l'intervento della Polizia Postale.

Inoltre quando le interazioni comunicative avvengono prevalentemente online avviene un generale indebolimento dell'empatia (capacità di sentire e capire come stanno gli altri), per cui si è portati a non provare emozioni simili per intensità a quelle che si proverebbero di persona di fronte ad un'ingiustizia. L'impossibilità di vedere con i propri occhi la sofferenza e l'umiliazione provate dalla vittima fa sì che il tutto venga percepito come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Il fenomeno a volte può essere sottovalutato anche dal mondo adulto.

Nei casi più gravi, il cyberbullismo può arrivare a distruggere la reputazione della vittima. Qualsiasi minore ultraquattordicenne può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Passate le 24 ore, se il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante della Privacy, che rimuoverà i contenuti entro 48 h.

Purtroppo ci sono delle tendenze e convinzioni nell'uso della Rete che complicano la gestione di queste situazioni: ad esempio la percezione che online non ci siano norme sociali da rispettare o che, per i più giovani, la Rete sia il luogo per eccellenza dove mettersi in gioco e fingere di essere ciò che non si è, dove simulare giochi di ruolo.

Sono proprio gli spettatori che invece possono fare la differenza, perché la responsabilità è condivisa e il gruppo ha il potere di denunciare/ fermare una situazione di cyberbullismo.

E' proprio sulla costruzione di profili di cittadinanza digitale attiva e responsabile che la scuola deve investire moltissimo, dal momento che è solo attraverso la formazione di giovani consapevoli e attenti che è possibile arginare la piaga del cyberbullismo.

4.3 - Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Tale fenomeno è particolarmente diffuso e insidioso, non meno grave della sua espressione offline, ma più difficile da individuare e combattere. Purtroppo la diffusione di messaggio di incitamento all'odio è maggiormente tollerata in Internet, che è meno sottoposto a controlli. Il discorso d'odio procura sofferenza in chi lo subisce e ha indubbiamente radici profonde, che devono essere individuate e "smantellate".

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono un ruolo centrale per la promozione della consapevolezza di queste dinamiche in Rete.

Il nostro Istituto si impegna a fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si formano forme di hate speech e promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e il social network.

4.4 - Dipendenza da Internet e gioco online

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

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale? La scuola può insegnare molto da questo punto di vista, se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionante che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.

In collaborazione con il Referente Salute dell'Istituto, si possono fare - come già avvenuto - incontri di formazione per gli studenti sulla ludopatia e le dipendenze.

In classe si possono creare altresì momenti di riflessione personale e comunitaria, ponendo nel gruppo domande su come e quanto si trascorre il tempo online, che valore e significato assume questo tempo nella loro quotidianità, se i videogiochi a cui accedono sono adeguati all'età, se ci sono atteggiamenti che si possono cambiare per incrementare il benessere personale, interrogandosi su quale ruolo vogliamo che abbia la tecnologia nella nostra vita.

A tal proposito, ad esempio, si possono invitare le famiglie a condividere coi propri figli semplici e chiare regole di utilizzo di videogiochi e dispositivi digitali.

La nostra scuola è convinta che se controlliamo la tecnologia, possiamo usarne appieno il potenziale e trarne gli indubbi vantaggi.

4.5 - Sexting

Il “sexting” è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video. Tra le conseguenze dirette di questo fenomeno vi sono:

- la *fiducia tradita*, di chi produce e invia contenuti sessualmente espliciti senza pensare alle conseguenze di tali gesti;

- la *pervasività* con cui si possono diffondere tali contenuti, sfuggendo rapidamente a qualsiasi controllo;

- la *persistenza* del fenomeno nel tempo, che potrebbe rimanere accessibile per sempre o essere difficilmente rimosso.

I rischi del sexting sono innumerevoli, dal revenge porn alla violenza psicosessuale, dall'umiliazione al bullismo/cyberbullismo, alle molestie e allo stress emotivo che può tramutarsi rapidamente nei soggetti coinvolti in stati diffusi d'ansia, sfiducia nell'altro, depressione.

Lo scambio di foto/video a sfondo sessuale, anche di se stessi, è un comportamento inquadrabile alla luce dell’esplorazione e dell’espressione della sessualità dei ragazzi, che iniziano a scoprirsi e viversi come dei giovani adulti. Nella maggior parte dei casi, la motivazione riportata rispetto all’invio di foto a terzi è quella del gioco, della richiesta di attenzione, della provocazione, fino alla “prova d’amore”. L'invio di questo materiale, purtroppo, spesso è messo in atto seguendo l’impulso e senza pensare alle possibili conseguenze.

La scuola e la famiglia devono informare con delicatezza di questo fenomeno (con la dovuta gradualità) i minori, in un contesto adeguato, in maniera tranquilla e non inquisitoria, facendo capire chiaramente i rischi connessi al fenomeno, per ridurne le molteplici conseguenze. In caso di evidenza, va valutata l'opportunità di rivolgetevi alla Polizia Postale e delle Comunicazioni o al Telefono Azzurro.

In generale, sarebbe auspicabile che le famiglie instaurassero un dialogo costruttivo e sereno sulla sessualità con i propri figli, sui cambiamenti del corpo, sullo sviluppo e l’identità sessuale.

Allo stesso modo, la scuola predispone sia alla fine della scuola primaria che durante la secondaria un percorso di educazione affettiva e sessuale, in collaborazione con lo psicologo d'Istituto, che poi si impegna, in un incontro collettivo, a restituire le principali evidenze emerse alle famiglie.

4.6 - Adescamento online

Il ***grooming*** (dall’inglese “groom” - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento. Avere un profilo sui social network significa accedere ad un bacino molto ampio di conoscenze virtuali che non si conoscono direttamente nella vita reale. Contare tanti amici online o molti follower è sinonimo di popolarità e per questo gli adolescenti aggiungono spesso alla propria cerchia in Rete numerosi "amici di amici", senza essere pienamente consapevoli del fatto che in questo modo stanno dando accesso a una grande quantità di informazioni private: luoghi che frequentano, foto e molto altro. Questo li espone potenzialmente a rischi importanti, perché queste informazioni possono essere utilizzate dagli sconosciuti in modo inaspettato e con ripercussioni negative nella vita reale.

Aiutare ragazzi e adolescenti a *proteggersi sul web* scegliendo con cura chi frequentare online è quindi un compito importante degli adulti che li circondano, a partire da genitori e insegnanti, per tutelarli nella vita reale.

Conoscere bene il fenomeno e le fasi dell'adescamento in rete (amicizia iniziale, risk assessment, costruzione del rapporto di fiducia, esclusività e sessualizzazione della relazione) è un primo passo per raggiungere con successo questo obiettivo.

Per gli adulti di riferimento, in particolare per i genitori, la comunicazione con i ragazzi è il primo strumento per accorgersi che qualcosa non va. Tuttavia potrebbe non essere sufficiente. I ragazzi potrebbero sentirsi troppo colpevoli per aprirsi, o non rendersi conto di essere vittime di un abuso. A questo punto il saper riconoscere la situazione a rischio diventa cruciale.

In caso di adescamento di minorenni online, rivolgersi prima possibile alla Polizia Postale ad altri presidi di Polizia (Questura, Commissariati di Polizia di Stato o Caserme dei Carabinieri). Se si percepisce un rischio per il benessere psicofisico delle persone minorenni coinvolte è bene rivolgersi ad un servizio di supporto psicologico anche passando per una consultazione presso i servizi territoriali di riferimento (Consultori Familiari, Servizi di Neuropsichiatria infantile).

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad*

esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - *Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.*

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere. La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **"Segnala contenuti illegali"** (Hotline).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

Proteggere i nostri ragazzi dalla pedopornografia non significa cominciare a controllare ogni singolo contenuto dei cellulari dei nostri adolescenti, ma occuparci del loro mondo, "riducendo le distanze".

Il dialogo e la condivisione di regole (adeguate all'età) sull'uso delle tecnologie sono fondamentali per un'educazione positiva all'utilizzo delle tecnologie e la prevenzione deve cominciare presto, prestissimo, dato che viviamo circondati dalle tecnologie digitali: siamo onlife, le nostre vite online e offline sono connesse.

Essere consapevole dei rischi che si annidano online, è un primo importante passo per navigare con coscienza e saper riconoscere un pericolo. Secondo una recente indagine Ipsos realizzata per Save the Children (gennaio 2020), "Minori e percezione dei rischi", genitori e ragazzi considerano lo spazio "virtuale" come il meno sicuro. La rete è infatti un luogo a rischio per l'85% degli adulti e il 74% dei ragazzi intervistati.

Supportare bambini e adolescenti nella gestione della propria identità online è fondamentale per gli adulti di riferimento. Parlare, interessarsi e prevenire sono le parole chiave per evitare di trovarsi coinvolti in situazioni rischiose. Gli studenti più grandi dovrebbero essere supportati nel riconoscimento e nella gestione delle proprie emozioni, nello sviluppo di autonomia, responsabilità e senso etico. Devono imparare ad esercitare il proprio

VIIC82800V - REGISTRO PROTOCOLLO - 0008261 - 22/11/2021 - E4 - U
pensiero critico anche quando sono online, quando cioè provare empatia per l'altro è più difficile, perché scatta un meccanismo di de-responsabilizzazione e di distacco. Devono sapere che se si ritrovano in una situazione più grande di loro, possono chiedere aiuto e possono chiederlo e riceverlo anche se si sono messi nei guai.

In particolare, segnalare materiale pedopornografico rinvenuto online è importantissimo. Segnalare consente alle forze dell'ordine di investigare al fine di individuare non solo chi produce, detiene e condivide questo materiale ma, soprattutto, di identificare i minori presenti nelle immagini e nei video e assicurare loro la protezione e il supporto necessari.

Il nostro piano d'azione

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

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

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

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

Firmato digitalmente da MARIA CATENA PALMINA OLIVIA LUPO

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'e-Policy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'e-Policy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso**.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un

VIIC82800V - REGISTRO PROTOCOLLO - 0008261 - 22/11/2021 - E4 - U
"pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Sexting: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

Nel caso a scuola gli insegnanti notassero o fossero informati di alcuni comportamenti non responsabili o potenzialmente pericolosi posti in essere da uno o più studenti, può rendersi necessaria una convocazione dei genitori o una relazione scritta al Dirigente Scolastico il quale valuterà le possibili azioni conseguenti.

Inoltre il nostro istituto offre sul sito e in allegato a questo documento una scheda per la segnalazione della violazione a Garante per la Privacy.

Riconoscere e intervenire in situazioni di bullismo e cyberbullismo non è semplice.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei

Firmato digitalmente da MARIA CATENA PALMINA OLIVIA LUPO

contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo. Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Disporre di adeguati strumenti condivisi da tutta la scuola è fondamentale per affrontare in modo sistematico le criticità.

E' importante che a scuola, in tutti i plessi, siano facilmente reperibili la scheda di Osservazione per fenomeni afferenti a bullismo e cyberbullismo e la scheda per la Segnalazione del presunto caso di bullismo e cyberbullismo.

La compilazione degli stessi, da parte della persona coinvolta o per mano di terzi, è il primo passaggio per una corretta gestione di un eventuale problema. E' altresì possibile comunicare direttamente con gli insegnanti della Commissione Bullismo, con la psicologa dello sportello di spazio-ascolto, la vicepreside o il Dirigente Scolastico, che si faranno da tramite.

Conservare le prove, è utile per fornire elementi utili a cercare di comprendere l'accaduto. Eventuali testimonianze dirette o indirette, devono comunque essere comunicate alla Commissione Bullismo, che deciderà come procedere.

Quando si viene a conoscenza di un problema di bullismo e cyberbullismo non è opportuno che il singolo intraprenda iniziative personali, come ad esempio interrogare bulli e/o le vittime: occorre rivolgersi alla Commissione che, progettando l'intervento e confrontandosi anche con i docenti di classe, prenderà in carico il problema.

La segnalazione alle autorità competenti può avvenire su iniziativa della famiglia del minore coinvolto o può essere fatta dalla scuola.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

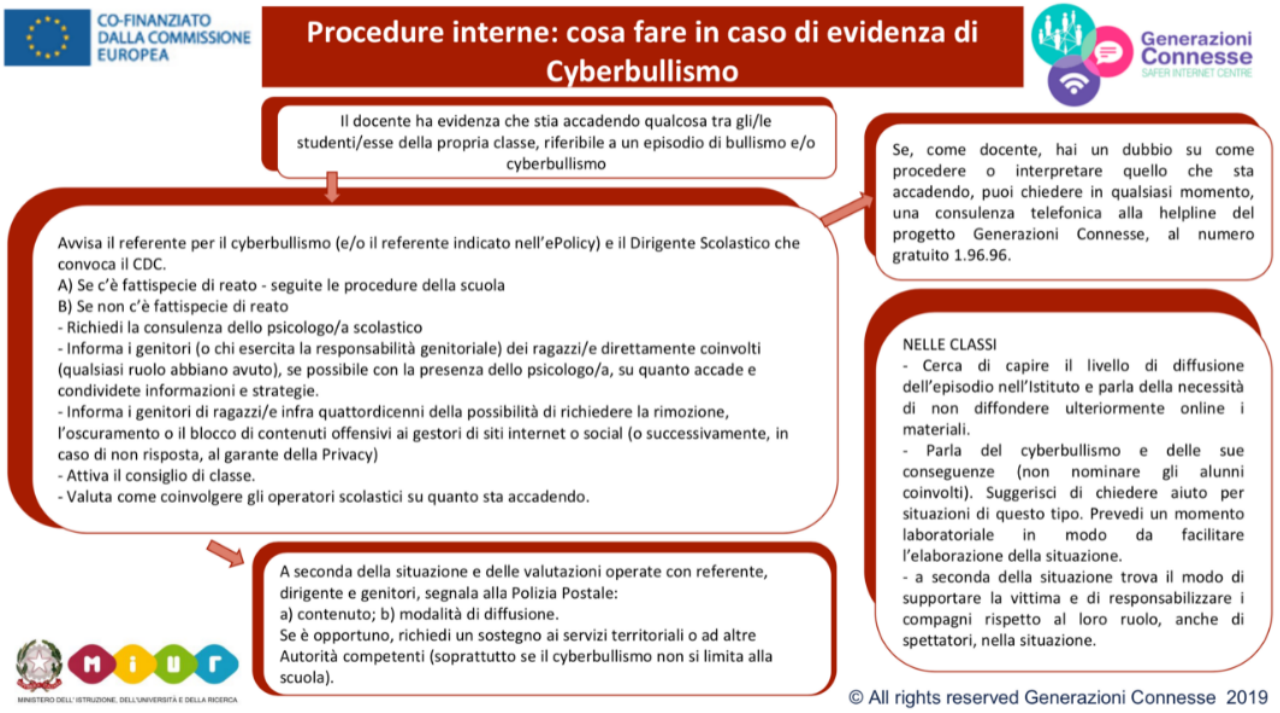
Le risorse del territorio hanno valenza educativa e formativa e vanno attentamente considerate in un'ottica di cooperazione e integrazione di servizi nonché di corresponsabilità.

E' importante costruire alleanze con le famiglie e col territorio che non si limitino a rapporti fugaci, negli eventuali momenti più critici o dettati dall'emergenza, ma che facciano parte di un progetto chiaro, trasparente e condiviso.

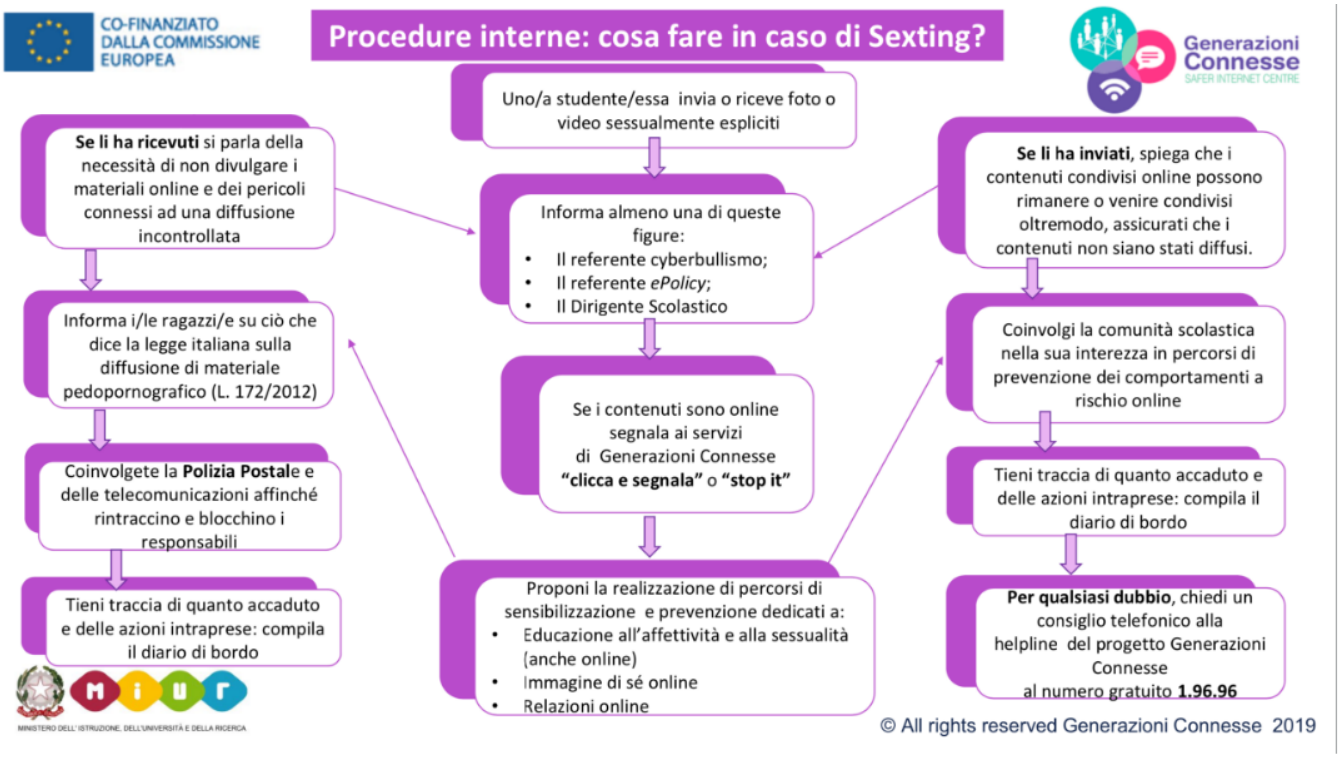
L'Ufficio Scolastico Provinciale e la Regione Veneto, oltre ad essere attivi con proposte di formazione e incontri con gli enti sul territorio, hanno prodotto nel mese di ottobre 2021 un VADEMECUM per la prevenzione al Bullismo e al Cyberbullismo, che a breve potrà essere disponibile sul sito della Regione.

5.4. - Allegati con le procedure

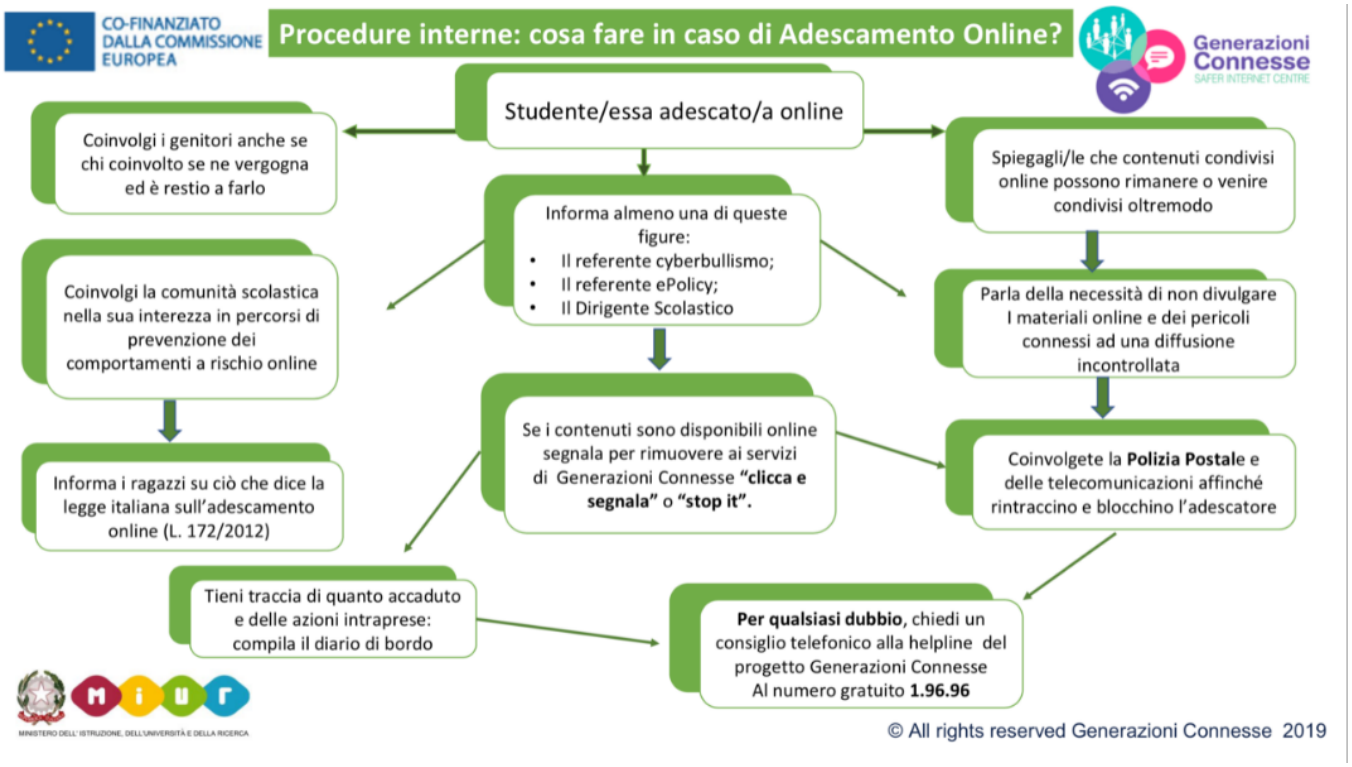
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



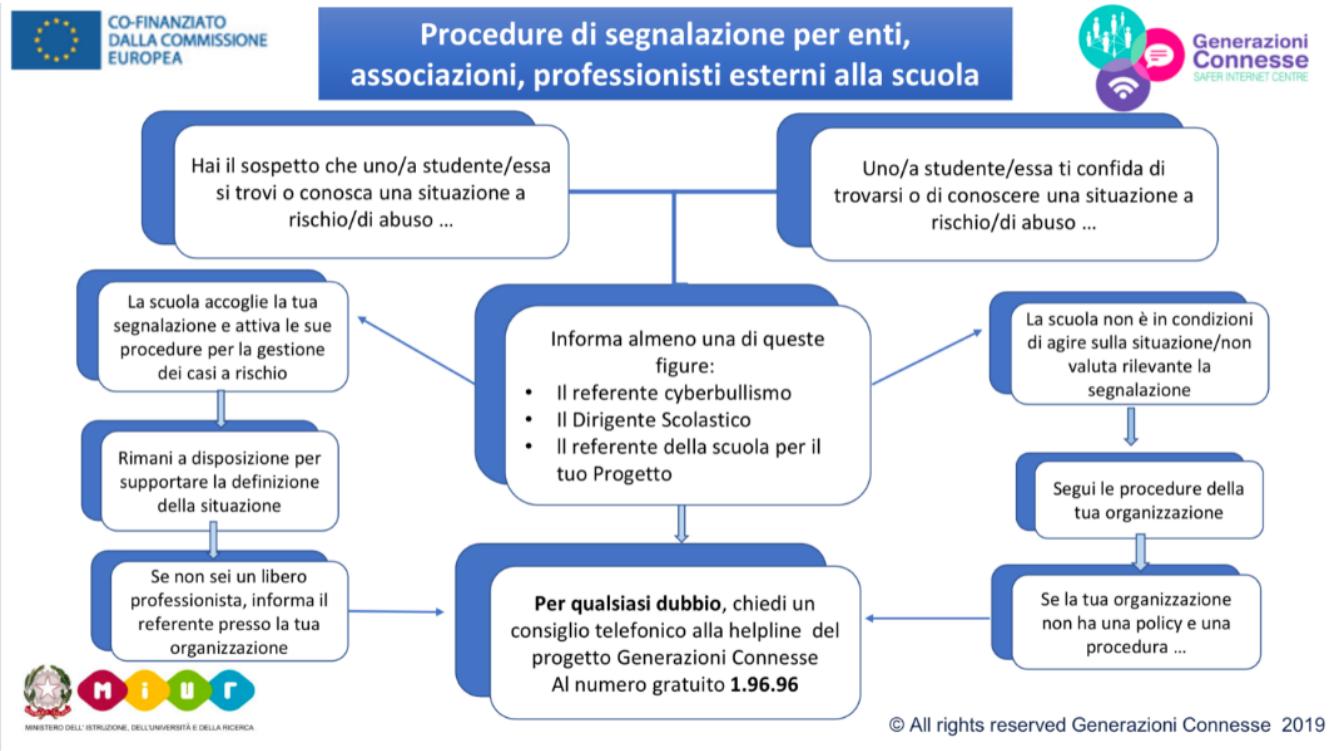
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Altri allegati

1. **GESTIONE DEI CASI: IL PROTOCOLLO D'AZIONE DELL'IC VALDAGNO 1**
2. **SCHEDA DI OSSERVAZIONE PER LA RILEVAZIONE DI EVENTUALI SITUAZIONI PROBLEMATICHE IN CLASSE RICONDUCIBILI A BULLISMO /CYBERBULLISMO**
3. **SCHEDA DI SEGNALAZIONE SITUAZIONE DI BULLISMO/CYBERBULLISMO**
4. **MODELLO PER LA SEGNALAZIONE AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**
5. **5. P.U.A. (POLITICA DI USO ACCETTABILE IN MERITO ALLA SICUREZZA INFORMATICA ED USO CONSAPEVOLE DELLE T.I.C NELLA SCUOLA)**

---

1. GESTIONE DEI CASI: IL PROTOCOLLO D'AZIONE DELL'IC VALDAGNO 1

La nostra scuola ha approvato un protocollo d'azione in quattro fasi per la segnalazione e la presa in carico di situazioni problematiche:

1- RICEZIONE DELLA SEGNALAZIONE. La ricezione e l'accoglienza da parte della scuola di una segnalazione di atti di bullismo e cyberbullismo coincide con la presa in carico di essa da parte del nostro Istituto. Ascolto e garanzia di riservatezza, ove possibile, sono d'obbligo. Generalmente in questa fase è già possibile individuare se si tratta di bullismo/cyberbullismo. La scuola è presente e vicina a chiunque chieda un suo intervento, poiché il benessere della comunità scolastica è una dimensione fondamentale.

2. VALUTAZIONE DELLA SEGNALAZIONE. La segnalazione viene presa in carico dalla Commissione Bullismo. In questa fase possono essere effettuati accertamenti e/o intrapresi, da uno psicologo interno alla scuola o da docente esperto, dei colloqui individuali con le persone coinvolte, nel rispetto della loro privacy e nell'ottica di un'alleanza terapeutica.

La Commissione si riserva di informare la famiglia nel caso di una situazione di effettivo pericolo.

In questa fase si classificheranno le segnalazioni in base alla loro specifica natura, ovvero secondo la tipologia "dell'immaturità", "della prepotenza e della prevaricazione (bullismo)", "delle molestie/offese attuate attraverso strumenti tecnologici (cyberbullismo)" o "degli abusi".

3. SCELTA DI INTERVENTO E GESTIONE DEL CASO. La Commissione, in accordo con i coordinatori di classe può valutare se è opportuno gestire il caso individualmente, nel gruppo classe o in piccolo gruppi, alla presenza o meno degli alunni coinvolti, a seconda della linea che si decide di seguire.

Qualora la scuola rilevi una situazione psico-socio-educativa particolarmente problematica, si riserva di convocare i genitori per valutare con loro a quali risorse territoriali rivolgersi. La scuola, se ne ravvede la necessità, può consigliare le persone coinvolte di rivolgersi allo sportello di spazio-ascolto psicologico dell'Istituto o può supportare la richiesta delle famiglie presso i Servizi Sociali dell'ULSS per la fruizione di servizi socio educativi comunali e all'ASL di competenza per altri interventi di natura psicologica e psicoterapeutica (Pediatria, Neuropsichiatria, Consultorio Familiare).

4. MONITORAGGIO. E' opportuno che, a distanza di due settimane e di due mesi dalle azioni intraprese dalla scuola, venga pensata un'attività di monitoraggio della situazione e del problema segnalato.

---

2. SCHEDA DI OSSERVAZIONE PER LA RILEVAZIONE DI EVENTUALI SITUAZIONI PROBLEMATICHE IN CLASSE RICONDUCIBILI A BULLISMO /CYBERBULLISMO

ISTITUTO COMPRENSIVO VALDAGNO 1
Via Pasubio 171 – 36078 Valdagno (VI) - Tel. 0445-410428 – Fax 0445-426014
Indirizzi mail: viic82800v@istruzione.it – P.E.C.: viic82800v@pec.istruzione.it
Sito web: www.icvaldagno1.edu.it

SCHEDA DI OSSERVAZIONE PER LA RILEVAZIONE DI EVENTUALI SITUAZIONI PROBLEMATICHE IN CLASSE RICONDUCIBILI A BULLISMO/ CYBERBULLISMO

PER L'ALUNNO/A _____

1° segnalazione. Il problema è stato osservato da……

Data…… Luogo …….. Orario:……

Nome di chi ha subito:……..…… Nome di chi ha agito:……..

Descrizione del comportamento/della situazione: ……

……

……

(Eventuale) comportamento/reazione della classe: ……

……

Azione messa in atto dall'adulto: ☐nessuna ☐richiamo ☐ intervento in classe ☐ nota sul libretto
☐nota sul registro ☐telefonata/ convocazione della famiglia

Attualmente il rendimento scolastico dell'alunno che ha subito risulta ☐ stabile ☐ in calo

Il suo livello di attenzione/partecipazione in classe è ☐invariato ☐ alterato ☐ molto alterato

3. SCHEDA DI SEGNALAZIONE PER PRESUNTO CASO DI BULLISMO/CYBERBULLISMO

Generazioni Connesse SAFER INTERNET CENTRE

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Co-financed by the European Union
Connecting Europe Facility

MODULO PER LA SEGNALAZIONE DI CASI

Nome di chi compila la segnalazione:	Ruolo:
Data:	Scuola:

Descrizione dell'episodio o del problema		
Soggetti coinvolti	Vittima/e: 1..... Classe: .... 2..... Classe: .... 3..... Classe:	Autore/autrice e sostenitori: 1..... Classe: .... 2..... Classe: .... 3..... Classe: ....
Chi ha riferito dell'episodio?	- La vittima - Un compagno della vittima, nome: - Genitore, nome: - Insegnante, nome: - Altri, specificare:	
Atteggiamento del gruppo	Da quanti compagni è sostenuto il bullo? Quanti compagni supportano la vittima o potrebbero farlo?	
Gli insegnanti sono intervenuti in qualche modo ?		
La famiglia o altri adulti hanno cercato di intervenire ?		
Chi è stato informato della situazione?	☐ coordinatore di classe data: ☐ consiglio di classe data: ☐ dirigente scolastico data: ☐ la famiglia della vittima/e data:	☐ la famiglia del bullo/i data: ☐ le forze dell'ordine data: ☐ altro, specificare:

MODULO PER IL FOLLOW-UP DEI CASI

Generazioni Connesse
SAFER INTERNET CENTRE

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Co-financed by the European Union
Connecting Europe Facility

	AZIONI INTRAPRESE	La situazione è
Aggiornamento 1		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 2		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 3		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 4		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 5		☐ migliorata ☐ invariata ☐ peggiorata Come:

4. MODELLO PER LA SEGNALAZIONE AL GARANTE DELLA PRIVACY IN MATERIA DI CYBERBULLISMO

Al Garante per la protezione dei dati personali

Inviare all'indirizzo e-mail: cyberbullismo@gpdp.it

OGGETTO: segnalazione ai sensi dell'art.2, comma 2, legge 29 maggio 2017, n.71, disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo.

Il/La sottoscritto/a _____(1), nato/a a _____,
il _____, residente a _____, via/p.za _____, tel. _____,
e-mail/PEC _____ [inserire recapiti ai quale si può essere contattati e selezionare, di seguito, l'opzione pertinente], minore ultraquattordicenne,

ovvero

in qualità di esercente la responsabilità genitoriale sul minore _____, nato a _____ il _____.

SEGNALA

1. di essere stato/a vittima ovvero che il minore sul quale esercita la responsabilità genitoriale è stato vittima di cyberbullismo [eliminare la locuzione che non interessa]. In particolare, i comportamenti posti in essere, realizzati per via telematica e di seguito sinteticamente descritti, consistono in [selezionare la/e fattispecie rilevanti]

pressione

aggressione

molestia

ricatto

ingiuria

denigrazione

diffamazione

furto d'identità

alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati

ovvero

diffusione di contenuti on line aventi ad oggetto il minore ovvero uno o più componenti della famiglia del minore [rimuovere l'informazione non rilevante] allo scopo intenzionale e predominante di isolare il minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo.

Riferisce sinteticamente i seguenti fatti:

_____
_____
_____
_____
_____

che la diffusione di contenuti lesivi dell'interessato/a è avvenuta [selezionare la casella pertinente]:

sul sito internet _____ all'indirizzo web [necessario indicare URL]

_____

social media [necessario inserire individuazione univoca] _____ altro [necessario

specificare] _____

Allega i seguenti documenti (ad es. immagini, video, screenshot, etc.):

_____ _

_____ _

_____ _

Tanto premesso, [selezionare l'opzione pertinente]

considerato che il gestore del sito internet o del social media al quale è stata presentata l'istanza allegata per l'oscuramento, la rimozione o il blocco dei dati personali diffusi in internet non ha comunicato entro 24 ore di avere assunto l'incarico di

VIIC82800V - REGISTRO PROTOCOLLO - 0008261 - 22/11/2021 - E4 - U

provvedere all'oscuramento, alla rimozione o al blocco richiesto, né vi ha provveduto entro quarantotto ore [allegare la pertinente documentazione];

considerato che non è stato in grado di presentare un'istanza per l'oscuramento, la rimozione o il blocco dei dati personali diffusi in internet al gestore del sito internet o del social media non essendo possibile identificare il titolare del trattamento o il gestore del sito internet o del social media,

RICHIEDE

di disporre, ai sensi degli articoli 2, comma 2, l. n. 71/2017 nonché 143 e 144, d.lgs. n. 196/2003, il blocco/divieto della diffusione dei dati personali sopra descritti.

Il/La sottoscritto/a dichiara inoltre di [selezionare la casella pertinente]:

aver presentato denuncia/querela per i fatti sopra descritti presso _____;

non aver presentato denuncia/querela per i fatti sopra descritti.

ACCONSENTE

Ai sensi e per gli effetti degli articoli 13 e 23 del D.Lgs. 196/03, con la sottoscrizione del presente modulo, al trattamento dei dati personali qui forniti.

Luogo, data Nome e Cognome

_____ _____

1 Avvertenza: la segnalazione o il reclamo può essere presentata direttamente anche da minori d'età ultraquattordicenni ovvero da chi esercita la responsabilità genitoriale. Pertanto si prega il segnalante/reclamante di fornire le pertinenti informazioni.

Firmato digitalmente da MARIA CATENA PALMINA OLIVIA LUPO

5. P.U.A.(POLITICA DI USO ACCETTABILE IN MERITO ALLA SICUREZZA INFORMATICA ED USO CONSAPEVOLE DELLE T.I.C NELLA SCUOLA)

PUA
Politica di Uso Accettabile

-

Integrazione al Regolamento di Istituto

in merito alla Sicurezza Informatica

ed Uso Consapevole delle TIC nella scuola.

Introduzione e processo di revisione

L'Istituto Comprensivo Valdagno 1 si è dotato di una politica d'uso accettabile e responsabile di Internet per essere pronto a cogliere i cambiamenti sociali, economici, culturali e tecnologici del contesto in cui opera, in particolare per quanto riguarda la formazione dei cittadini del futuro, destinati a vivere in un ambiente in cui tutto viene gestito attraverso l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC). Tali tecnologie diventano abilitanti, quotidiane, ordinarie, al servizio dell'attività scolastica e di tutti i suoi ambienti. Il curricolo scolastico prevede che gli studenti imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le TIC.

L'Istituto inoltre intende utilizzare internet per promuovere l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione.

Poiché esiste la possibilità che gli studenti trovino materiale inadeguato e illegale su Internet, l'Istituto prende le precauzioni necessarie per evitare tali inconvenienti. Gli insegnanti hanno il compito di guidare gli studenti verso un uso di Internet accettabile e responsabile.

L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l'età e la maturità degli studenti.

La PUA verrà revisionata e aggiornata annualmente, anche in base a eventuali variazioni delle dotazioni tecnologiche e dei protocolli dell'Istituto.

Scopo della PUA

Scopo del presente documento è quello di informare e rendere responsabile l'utenza al fine di garantire un uso corretto e consapevole delle apparecchiature informatiche in dotazione e in uso all'interno dell'Istituto, nel rispetto della normativa vigente, definendo una linea di condotta precisa e chiara cui tutti gli utenti debbano attenersi.

È pertanto fondamentale conoscere le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico e avere la consapevolezza dei rischi cui si è esposti ogni volta che si naviga in Internet: esiste, infatti, la possibilità che durante il

lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale. Pertanto l'Istituto promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.

Stato di fatto: spazi fisici e virtuali disponibili nell'Istituto

- La quasi totalità delle aule del nostro Istituto, della Scuola Primaria e Secondaria, sono dotate di LIM, e la connessione alla rete della Scuola e quindi a Internet rientra nella pratica didattica quotidiana. I plessi della scuola D'Infanzia, quelli della Scuola Primaria e l'edificio della Scuola Secondaria sono dotati di rete LAN con la connessione ad Internet, ed è attiva anche una rete wireless.

- Il registro elettronico è in uso sia alla scuola secondaria sia alla scuola primaria.

- Gli uffici di segreteria, seguendo la normativa vigente, stanno perseguendo l'obiettivo della completa dematerializzazione; si presta particolare attenzione al potenziamento delle attrezzature informatiche, al mantenimento e costante aggiornamento della rete informatica e al potenziamento dei servizi digitali scuola-famiglia-studente.

- è una priorità il rinnovo dei PC nei laboratori, così che la scuola possa essere dotata di un numero adeguato di PC utilizzabili con gli alunni.

- I docenti devono servirsi delle TIC nelle attività didattiche in modo motivato e consono agli obiettivi educativi e didattici, assumendosi il fondamentale compito di responsabilizzare gli studenti, per renderli consapevoli sull'importanza della salvaguardia di un bene comune, grazie alle corrette norme di utilizzo.

Strategie dell'Istituto per garantire la sicurezza delle TIC

L'Istituto prevede le seguenti strategie per garantire la sicurezza in Rete:

- analizzare il fabbisogno formativo dei docenti e promuovere corsi di formazione inerenti all'uso sicuro e responsabile delle TIC e del web, sia nell' ambito privato, sia scolastico;

- attuare, eventualmente in collaborazione con esperti esterni, incontri per presentare le modalità corrette di fruizione del web (età minima per iscrizione ai social network), il problema della tutela dei minori su Internet e sui social network, le problematiche e i rischi legati a bullismo, cyberbullismo e uso non responsabile del web, a genitori, familiari e alle persone interessate presenti sul territorio;

- informare sulle problematiche psico-pedagogiche correlate all'uso della Rete;

- monitorare periodicamente il sistema informatico, in particolare per ciò che concerne l'uso di Internet, cronologia, cookie;

- chiedere, al bisogno, l'intervento delle società informatiche che si occupano di manutenzione e assistenza dei dispositivi con azioni in loco o da remoto;

- utilizzare eventuali dispositivi esterni personali solo se preventivamente autorizzati dal docente responsabile e sotto la sua vigilanza;

- organizzare un sistema di monitoraggio di eventuali problemi riscontrati durante l'uso delle TIC o della Rete e prevedere piani d'azione per risolvere i più frequenti;

- evidenziare il divieto di adottare comportamenti contrari al presente regolamento e alla normativa vigente.

Nonostante l'Istituto si faccia carico di mettere in atto tutte le precauzioni necessarie per garantire agli studenti l'accesso a materiale appropriato, non è possibile evitare in modo assoluto che gli studenti incorrano in materiale indesiderato navigando su

VIIC82800V - REGISTRO PROTOCOLLO - 0008261 - 22/11/2021 - E4 - U

un computer dell'Istituto.

Linee guida di buona condotta degli utenti

Ferme restando le strategie sistematiche messe in atto dall'Istituto di cui al precedente paragrafo e quanto eventualmente previsto nel Regolamento di Istituto, ciascun utente connesso alla Rete deve

- rispettare il presente regolamento e la legislazione vigente;

- tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni digitali cui ha accesso;

- rispettare la *netiquette*, ovvero quell'insieme di regole condivise che disciplinano il rapportarsi tra utenti della Rete, in contatto attraverso siti, forum, mail, blog, newsgroup…

Di seguito si dettagliano i comportamenti da tenere distinguendo attività e utenti. *Docenti*

Durante l'attività didattica ogni docente può avvalersi degli strumenti a disposizione e deve:

- leggere, comprendere e aderire a questa e-Policy;

- aver cura degli strumenti in dotazione, in particolare spegnendoli correttamente o riponendoli nel luogo predisposto al termine del loro utilizzo;

- accedere al registro elettronico attraverso i propri dispositivi personali o dal PC presente in classe (in tal caso provvedere a compilare quanto di competenza e provvedere tempestivamente al corretto logout);

- installare e utilizzare solo software autorizzati;

- non spostare i dispositivi dell'Istituto in locali diversi senza informarne il responsabile;

- non salvare sui dispositivi utilizzati file contenenti dati personali e/o sensibili;

- illustrare agli alunni le regole di utilizzo contenute nel del presente documento e informarli delle eventuali sanzioni disciplinari previste dal regolamento di Istituto;

- premurarsi che l'accesso degli alunni alla Rete avvenga sempre sotto la propria supervisione, informarli sui rischi cui sono potenzialmente esposti e sul corretto uso della Rete (motori di ricerca, piattaforme online, classi virtuali);

- guidare gli alunni nelle ricerche online: fornire obiettivi chiari, proporre indirizzi web, parole chiave per la ricerca, prediligendo siti istituzionali, creati ad hoc per la didattica; vigilare, durante la navigazione, che tutti usino in modo corretto la Rete, fornendo costanti indicazioni su ciò che è richiesto dalla netiquette;

- segnalare ai responsabili l'uso di siti internet non compatibili con la politica educativa dell'Istituto.

Studenti

Durante l'attività didattica gli alunni devono:

- leggere, comprendere e aderire a questa e-Policy;

- accedere al laboratorio di informatica solo se accompagnati da docenti e seguire le indicazioni fornite in merito all'utilizzo delle TIC;

Firmato digitalmente da MARIA CATENA PALMINA OLIVIA LUPO

- accedere alla Rete solo in presenza e previa autorizzazione del docente responsabile dell'attività;

- utilizzare la strumentazione dell'Istituto solo per scopi didattici e non personali; - lasciare immutata la configurazione di sistema dei dispositivi;

- sono previste eccezioni per l'uso dei dispositivi da parte degli alunni con BES, per i quali è possibile l'utilizzo del PC personale e la registrazione delle lezioni, regolamentati dai rispettivi PEI e PDP e dalla normativa vigente.

- Inoltre, per specifiche attività didattiche organizzate da un docente di classe, è consentito l'uso a scuola di dispositivi personali

Genitori

I genitori sono tenuti a

- leggere, aderire, comprendere e promuovere l'ePolicy e la PUA con i loro figli

- controllare con regolarità il registro elettronico e il sito istituzionale dell'Istituto;

- confrontarsi con il personale dell'Istituto se dovessero sorgere preoccupazioni riguardo l'uso della tecnologia da parte del figlio

e sono invitati a

- monitorare il modo in cui i figli usano la tecnologia in ambiente extrascolastico e guidarli verso un comportamento responsabile e sicuro.

Altre tipologie di TIC

Lo studente non può utilizzare per scopi personali i device di sua proprietà nei locali scolastici e relative pertinenze.

L'eventuale utilizzo di dispositivi personali durante una specifica attività didattica, inserita nel PTOF, deve essere autorizzata e costantemente supervisionata dal docente di classe. Le infrazioni e le sanzioni relative a un uso improprio delle TIC da parte degli studenti sono declinate nel Regolamento d'Istituto e nell'ePolicy.

La *netiquette*

Chiunque si trovi a utilizzare le TIC, Internet e i servizi offerti dalla Rete deve attenersi a una serie di regole che disciplinano il comportamento degli utenti nel rapportarsi con gli altri; tali norme costituiscono la cosiddetta netiquette, una sorta di galateo della Rete. Si riportano alcune delle norme su cui si intende sensibilizzare in modo particolare l'utenza:

- in Rete la comunicazione avviene principalmente attraverso testi, con conseguente rischio di essere fraintesi; talvolta, nei contesti opportuni, le emoticon possono aiutare a chiarire il tono del messaggio; risulta opportuno quotare i messaggi originari per facilitare la comprensione delle risposte;

- evitare di inviare messaggi ripetitivi, inutili o inopportuni (spam); evitare altresì l'invio di messaggi pubblicitari, "catene" o comunicazioni non espressamente richieste;

- in Rete si possono esprimere la propria opinione e le proprie idee, sempre rispettando tutti gli interlocutori e i fruitori del messaggio; la Rete offre la possibilità di entrare in contatto con milioni di utenti, dei quali vanno rispettati la nazionalità, la cultura, la religione, il sesso; non sono ammesse forme di razzismo o discriminatorie;

- è necessario rispettare gli interlocutori virtuali: i loro tempi nella risposta, che non andrà mai pretesa, il loro interesse o meno a

quanto proposto; gli errori di digitazione, di grammatica o di sintassi non devono essere stigmatizzati, l'importante è che la trasmissione del messaggio avvenga con successo; si ricorda che lo scrivere in maiuscolo equivale a urlare: non abusarne;

- scegliere forum, social, community, chat, mailing list… cui si intende partecipare in base agli argomenti che interessano o alle esigenze emerse; partecipare rispettandone le regole e gli interventi dei moderatori;

- l'espressione del proprio parere deve avvenire in modo pacato, così da non provocare dure reazioni nelle persone con cui si comunica ed evitare "guerre di opinione";

- non utilizzare le proprie competenze digitali per violare siti o profili di altri utenti, pubblicare contenuti o conversazioni private, condividere fotografie, video o altri file di utenti terzi senza averne il consenso;

- curare la propria reputazione digitale, valutando sempre con la massima attenzione ciò che si vuole comunicare, pubblicare e condividere;

- rispettare la privacy degli altri utenti: ognuno può scegliere cosa pubblicare e cosa condividere delle informazioni che lo riguardano;

- evitare di rivelare dettagli, informazioni personali o dati sensibili propri o altrui;

- utilizzare la Rete con spirito critico: evitare di credere a tutto ciò che viene detto e diffidare di chi chiede informazioni personali o incontri dopo poco tempo che si è entrati in contatto perché non sempre è possibile avere la certezza dell'identità della persona con la quale si sta comunicando.

Comunicazione con l'Istituto

L'Istituto promuove una comunicazione chiara ed esplicita con il personale, le famiglie e il territorio, in particolare attraverso

- il sito istituzionale, costantemente aggiornato, che fornisce un'informazione puntuale e trasparente sulla documentazione e le attività relative all'Istituto;

- il registro elettronico, costantemente aggiornato dai docenti, sul quale le famiglie possono controllare assenze, voti, annotazioni (scuola secondaria) e schede di valutazione (scuola primaria e secondaria);

- la posta elettronica.

Garanzia e tutela della privacy

L'Istituto opera a ogni livello rispettando tutte le normative vigenti in merito alla tutela della privacy, come indicato sul sito istituzionale. Esistono liberatorie per il trattamento dei dati personali di genitori e studenti, del personale scolastico, degli studenti che accedono alla piattaforma di e-learnig in uso dalla scuola. Gli esiti degli esami e degli scrutini finali sono pubblici ed esposti in forma cartacea: l'Istituto si impegna, però, ad evitare di fornire, anche indirettamente, informazioni sulle condizioni di salute degli alunni, o altri dati personali non pertinenti.

Sportello d'ascolto

Tra le misure di prevenzione che l'Istituto mette in atto per la prevenzione del disagio, anche per quanto riguarda l'uso delle TIC, di Internet e le relazioni virtuali che nella Rete si possono sviluppare, si registra la presenza alla scuola secondaria di uno "Sportello di ascolto", rivolto a tutti gli allievi, articolato in colloqui individuali e/o collettivi, con l'obiettivo di migliorare il benessere personale e scolastico di ogni singolo alunno, mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale. È previsto, al suo interno, uno spazio riservato ai docenti e genitori al fine di individuare strategie efficaci per affrontare problematiche tipiche dell'età adolescenziale. L'Istituto si prodigherà nella tutela dei minori coinvolti, senza rendere in

VIIC82800V - REGISTRO PROTOCOLLO - 0008261 - 22/11/2021 - E4 - U

alcun modo identificabili, con dati o altri strumenti, gli stessi.

Didattica e azione dei docenti

L'Istituto, come evidenziato nel Piano Triennale dell'Offerta Formativa, pone particolare attenzione allo sviluppo della competenza digitale dei propri studenti, in linea con quanto previsto dal Piano Nazionale per la Scuola Digitale (PNSD). Questa competenza non può essere sciolta dalle competenze sociali e civiche che ogni alunno deve maturare, soprattutto per gli aspetti relazionali da esse implicati: l'ascolto, il rispetto reciproco, la capacità di vivere insieme. In tal modo ci si prefigge di prevenire eventuali fenomeni di disagio giovanile (bullismo, cyberbullismo, violenza, discriminazioni, uso di sostanze stupefacenti…). La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni, nonché per comunicare e partecipare a reti collaborative tramite Internet. Si pone quindi enfasi sulla capacità di esplorare e affrontare in modo flessibile situazioni tecnologicamente nuove, adeguando le performance ai diversi contesti in cui si opera.

L'Istituto, coerentemente con quanto previsto dal PNSD, attiva dei percorsi di formazione rivolti ai docenti per acquisire le competenze necessarie.

Prevenzione, rilevazione e gestione dei casi

L'Istituto si prefigge come obiettivo quello di fornire a tutta l'utenza le competenze necessarie al fine di tenere comportamenti responsabili e corretti nella fruizione delle TIC e della Rete, così da poter prevenire i rischi in cui ci si può imbattere. Per quanto riguarda l'uso delle TIC, il personale in servizio presso l'Istituto, gli alunni e le loro famiglie sono informati e formati in merito alle modalità per utilizzare in modo sicuro, negli ambienti scolastici o all'esterno, i diversi device, quali tablet, PC, smartphone, fornendo loro indicazioni su come gestire impostazioni di cronologia, cookie, cache, firewall, malware e virus in genere.

Tutte le componenti scolastiche, in particolare personale docente e genitori, devono essere formate, informate e aggiornate sui fenomeni del bullismo e del cyberbullismo.

A tal fine, presso il nostro istituto sono stati svolti negli ultimi anni percorsi formativi sull'argomento ed è stato nominato un Referente di Istituto per il contrasto al bullismo e al cyberbullismo, attivo con una Commissione. Inoltre è attivo il Team Antibullismo e il team per l'Emergenza, entrambi presieduti dal Dirigente Scolastico.

L'Istituto si impegna a formare e aggiornare i docenti sulle modalità e gli indicatori per riconoscere eventuali casi o situazioni a rischio e sulle procedure da seguire . Per ulteriori informazioni si rimanda all'omonimo paragrafo all'interno dell'e-Policy.

Diffusione della PUA

La PUA e le regole in essa contenute verranno approvate dal Collegio dei Docenti e dal Consiglio di Istituto e pubblicate online sul sito istituzionale dell'Istituto. Il personale scolastico è tenuto alla lettura e sottoscrizione della PUA, nonché allo sviluppo delle linee guida e all'applicazione scrupolosa delle istruzioni sull'uso sicuro e responsabile della Rete. Gli studenti sono informati dei contenuti della PUA attraverso il Patto di Corresponsabilità e costantemente supportati per un uso responsabile e consapevole delle TIC e della Rete. I genitori o i tutori sono invitati a prestare la massima attenzione ai principi e alle regole contenuti in questo documento; si richiede un impegno costante affinché siano rispettate anche in ambito extrascolastico, assistendo i minori nel momento dell'utilizzo della Rete e adottando tutti i sistemi di sicurezza per diminuire i possibili rischi della Rete

FIrma per presa visione del documento. L'alunno I genitori dell'alunno

_____ _____

Firmato digitalmente da MARIA CATENA PALMINA OLIVIA LUPO