Istituto Comprensivo di Casalpusterlengo

2017-2018 -2019

ESAFETY POLICY

Regolamento approvato:

- dal Collegio dei Docenti in data 16 gennaio 2018
- dal Consiglio di Istituto con Delibera n° 13 del 9 febbraio 2018

Dirigente scolastico

Pasqualina Lucini Paioni

UNIONE EUROPEA
FONDI STRUTTURALI EUROPEI
PON 2014-2020
MIUR
Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
Direzione Generale per interventi in materia di edilizia scolastica, per la gestione dei fondi strutturali per l'istruzione e per l'innovazione digitale
Ufficio IV
PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO (FSE-FESR)

M.I.U.R.

Istituto Comprensivo di Casalpusterlengo ad Indirizzo Musicale

Via Olimpo, 6 26841 CASALPUSTERLENGO (LO)

Codice Meccanografico LOIC80900D Codice Fiscale 90518620159 Codice Univoco Ufficio UFTH6W

Tel. 037781940 – 037784379 E-Mail: loic80900d@istruzione.it PEC loic80900d@pec.istruzione.it
www.iccasalpusterlengo.edu.it

INTRODUZIONE

L'Istituto Comprensivo di Casalpusterlengo e l'intera comunità scolastica condannano severamente ogni atto di bullismo e di cyberbullismo così come vengono configurati dalla nuova legge (Legge 29 maggio 2017 n. 71) che per la prima volta stabilisce una definizione ufficiale di cyberbullismo: «qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito dei dati personali in danno di minorenni, nonché la diffusione di contenuti online 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».

È fondamentale che l'approccio al problema sia integrato e sistemico ossia debba coinvolgere l'intera comunità scolastica e territoriale che si deve aprire al confronto con esperti per capire come approfondire o risolvere i casi più complessi suggerendo ai minori coinvolti e alle loro famiglie, se lo richiedono, l'eventuale supporto necessario.

A tale scopo, l'I.C. Casalpusterlengo ha concordato con tutte le componenti della comunità scolastica e territoriale che partecipano al piano di prevenzione un documento programmatico che detta le linee strategiche mirate a contrastare i fenomeni del bullismo e del cyberbullismo: la policy e-Safety.

SCOPO DELLA POLICY

Lo scopo della e-Safety Policy è dotare il nostro Istituto di un insieme di regolamenti, linee di azioni e attività per far fronte ad una serie di bisogni individuati nella comunità scolastica:

- le misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici.
- le misure di prevenzione e misure di gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

RISCHI	MISURE DI PROMOZIONE	MISURE DI PREVENZIONE
esposizione a contenuti inappropriati; visita di siti web inappropriati validazione dell'affidabilità, dell'autenticità e dell'esattezza dei contenuti online; copyright (poca cura o considerazione per i diritti d'autore relativamente a musica, film, immagini); bullismo on-line in tutte le forme; questioni di privacy, tra cui la divulgazione di informazioni personali; reputazione on-line; la salute e il benessere (quantità di tempo speso online su Internet o giochi); sexting (invio e ricezione di immagini personali intime).	Uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet.	Salvaguardare e proteggere gli studenti e il personale dell'Istituto.
	Far acquisire le procedure e le competenze "tecniche" delle TIC.	Prevenire attraverso azioni di contrasto i fenomeni di cyberbullismo
	Impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile delle TIC.	Garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e sanzionabile con opportune azioni disciplinari e giudiziarie.
	Attivare un supporto agli studenti vittime o spettatori attivi e/o passivi di casi di cyberbullismo.	Assistere il personale della scuola affinché possa lavorare in modo sicuro e responsabile con le tecnologie della comunicazione.
	Gestire situazioni problematiche relative all'uso delle tecnologie digitali.	Monitorare i propri standard e le prassi d'uso delle tecnologie.

RUOLI E RESPONSABILITÀ (CHE COSA CI SI ASPETTA DA TUTTI GLI ATTORI DELLA COMUNITÀ SCOLASTICA)

RUOLO	RESPONSABILITA'
Il Dirigente Scolastico è il titolare del trattamento di dati personali secondo la Legge sulla privacy (art. 41 f del D. Lgs. 196/2003) e **garantisce**	• la responsabilità per i dati e la sicurezza dei dati attraverso un Internet Service filtrato conforme ai requisiti di legge; • la formazione dei docenti volta a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie; • la formazione del personale preposto affinché riceva una preparazione adeguata per svolgere i ruoli di sicurezza on-line e per formare altri colleghi; • l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on line; • l'applicazione delle procedure previste dalle norme in caso di reclami; • l'attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.
Il direttore dei servizi generali e amministrativi (DSGA) in collaborazione con la Commissione sicurezza, l'animatore digitale, il pronto soccorso tecnologico e con il team digitale **assicura e garantisce**	• nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni; • Il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet; • le azioni opportune affinché tutto il personale sia a conoscenza delle procedure da seguire per garantire la sicurezza on-line; • la tenuta di un registro di incidenti di sicurezza online.

L'animatore digitale, il pronto soccorso digitale, il team digitale e la Commissione preposta al Progetto "Ondamedia" **<u>assicurano</u>**	• la formazione interna – in termini di risorse- all'istituzione negli ambiti di sviluppo della "scuola digitale"; • la consulenza e le informazioni al personale in relazione ai rischi on line e alle misure di prevenzione e di gestione degli stessi; • il monitoraggio e la rilevazione delle problematiche emergenti inerenti all'utilizzo sicuro delle tecnologie digitali e di internet; • la proposta di revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola; • l'accesso degli utenti alla rete della scuola solo tramite password applicate e regolarmente cambiate; • la partecipazione della comunità scolastica (alunni, genitori e altri attori del territorio) ad attività e progetti attinenti la "scuola digitale; • la pubblicazione della e-Safety Policy sul sito della scuola; • la diffusione della e- Safety Policy all'interno della comunità e della istituzione scolastica; • la tutela di tutti i dati relativi agli alunni pubblicati sul sito; • l'anonimato dei dati di alunni e genitori che accedono allo Sportello di Ascolto o alle attività relative al Progetto "Ondamedia" ove necessario; • il controllo dei contenuti pubblicati sul sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
La ditta incaricata della gestione tecnica del sito, <u>cura</u>	• la manutenzione e lo sviluppo del sito web della scuola nel rispetto delle norme previste per legge.

I docenti in collaborazione con ogni figura educativa che li affianca **<u>promuovono</u> e/o <u>garantiscono</u>**	• la presenza di tematiche legate alla sicurezza on-line in tutti gli aspetti del curricolo di studi e di altre attività scolastiche; • le modalità di utilizzo corretto e sicuro delle TIC e di internet nel curriculum di studio e nelle attività didattiche ed educative delle classi; • la supervisione e la guida degli alunni durante le attività di apprendimento che coinvolgono la tecnologia on-line; • attività di apprendimento mirate ad acquisire le procedure corrette di ricerca on line e a comprendere le opportunità di ricerca offerte dalle tecnologie digitali e dalla rete; • l'educazione alla consapevolezza dei problemi legali relativi ai contenuti elettronici (leggi sul copyright, riservatezza dei dati personali trattati ai sensi della normativa vigente); • le modalità di utilizzo corretto e sicuro delle TIC e di Internet durante le attività didattiche ed educative, così come sono state definite dal regolamento di istituto e di classe; • la comprensione e il conseguente rispetto delle regole - da parte degli alunni -per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet; • azioni di controllo affinché le comunicazioni digitali dei docenti tra alunni e genitori siano effettuate da canali scolastici ufficiali e nel rispetto del codice di comportamento professionale; • il controllo nell'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito); • l'utilizzo guidato di Internet, di siti controllati e verificati come adatti qualora sia consentito;

	• la comunicazione ai genitori di difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo; • la segnalazione di qualsiasi problema o proposta di carattere tecnico-organizzativo all'Animatore digitale per ricercare soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e per favorire un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC; • la segnalazione al Dirigente scolastico e ai genitori di qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, allo scopo di attivare le procedure previste dalle norme.
Gli alunni si assumeranno la responsabilità dei seguenti compiti:	• comprensione e conoscenza delle potenzialità e dei rischi di utilizzo di internet e di altre tecnologie sia a scuola che a casa; • acquisizione delle procedure di ricerca di contenuti e materiali, evitando il plagio e rispettando le normative sul diritto di autore; • adozione di buone pratiche di sicurezza on line quando si utilizzano tecnologie digitali fuori dalla scuola (gruppi, chat, messaggistica); • comprensione, conoscenza e sottoscrizione della e-Safety Policy nei seguenti ambiti: uso dei telefoni; fotocamere digitali; dispositivi portatili; • segnalazione di abusi, di uso improprio di materiale inappropriato; • conoscenza delle azioni da intraprendere nei casi di richieste di aiuto da parte di coetanei in difficoltà o particolarmente vulnerabili in situazioni di rischio on line fuori e dentro la scuola.

I genitori si assumeranno la responsabilità dei seguenti compiti:	• sostenere la scuola nel promuovere la sicurezza online e approvare controfirmando l'accordo di e-Safety Policy con la scuola. • accedere al sito web della scuola in conformità con quanto stabilito dalla stessa; • assicurarsi che la scuola abbia preso tutte le precauzioni necessarie circa un uso corretto della tecnologia da parte degli alunni. • seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc di internet, telefoni cellulari e device; • astenersi dal diffondere comunicazioni ufficiali della scuola attraverso canali digitali (chat, social, sms…); • controllare i contenuti delle chat on line dei propri figli allo scopo di prevenire e di risolvere eventuali situazioni di conflitto che possano avere una ricaduta negativa sulla vita scolastica degli studenti; • concordare con i docenti e gli organi collegiali le regole per l'utilizzo del computer e le linee di condotta per un uso responsabile delle tecnologie digitali o di internet.

CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA

La e-Safety Policy d'Istituto è condivisa da tutti i membri della scuola, compreso il personale, gli studenti, i genitori, gli utenti della comunità, che ne hanno accesso. La Policy sarà pubblicata sul sito della scuola previo accordo sottoscritto dal personale, dalle famiglie e dagli studenti tramite il Patto di Corresponsabilità.

ALUNNI	PERSONALE SCOLASTICO	GENITORI/COMUNITA' SCOLASTICA
• Utilizzo della rete, di Internet e di ogni dispositivo digitale solo sotto il controllo e la supervisione dei docenti. • Partecipazione a percorsi di apprendimento sulla e-Safety ai fini di aumentare la consapevolezza di un uso sicuro e responsabile di internet. • Condivisione delle regole (netiquette) sulla sicurezza online e successiva pubblicazione in tutte le aule e laboratori • Trattazione di temi particolarmente rilevanti concernenti la sicurezza e i rischi della navigazione online, sui comportamenti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili (cyberbullismo). • Costruzione di tutorial per facilitare la consultazione della e-Policy da parte delle famiglie.	• Discussione negli organi collegiali (consigli di interclasse/intersezione/classe, collegio dei docenti e consiglio di istituto) della e-Safety; condivisione e comunicazione ufficiale del documento a tutto il personale anche sul sito web. • Informazione mirata a rendere consapevole il personale che il traffico in internet può essere monitorato per risalire al singolo utente registrato. • Informazione/formazione on line del personale docente sull'uso sicuro e responsabile di internet attraverso corsi di formazione on line e in presenza. • Supervisione da parte dell'animatore digitale sul sistema di filtraggio adottato e sul monitoraggio relativo all'utilizzo delle TIC ed eventuale segnalazione di problemi al DSGA (acquisti o interventi di tecnici). • Consapevolezza che comportamenti dissonanti con la linea di condotta stabilita dalla e-Safety sono sanzionabili.	• Pubblicazione di informazioni o di avvisi per le famiglie relativi alla sicurezza e all'uso delle tecnologie digitali e di internet sul sito web della scuola o in formato cartaceo. • Partecipazione ad incontri di informazione/formazione scuola/famiglia assembleari, collegiali e individuali per incoraggiare un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet. • Traduzione delle netiquette e del testo semplificato della e- Policy ad uso delle famiglie migranti. • Consultazione sul sito della scuola o sulle piattaforme di apprendimento da parte dei genitori di risorse utili per lo studio, di siti idonei ed educativi per gli alunni, di sistemi di filtraggio, messi a disposizione dall'animatore digitale o da docenti esperti.

GESTIONE DELLE INFRAZIONI ALLA POLICY

Infrazioni	Sanzioni	Interventi preventivi (educativi)
Alunni (in ambito scolastico)		
• L'Invio incauto o senza permesso di foto o di altri dati personali; • la condivisione di immagini intime o troppo spinte; • la comunicazione incauta e senza permesso con sconosciuti, con amici o con genitori; • il collegamento a siti web non indicati dai docenti; • il download di file video-immagini, clip musicali protetti da copyright.	Sono previsti da parte dei docenti provvedimenti disciplinari proporzionati all'età e alla gravità del comportamento, quali: • Il richiamo verbale; • il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante); • il richiamo scritto con annotazione sul diario/quaderno comunicazioni; • la convocazione dei genitori da parte degli insegnanti; • la convocazione dei genitori da parte del Dirigente scolastico; • Ritiro del cellulare o di altri dispositivi e consegna al personale preposto della Segreteria.	Gli interventi di carattere educativo e preventivo saranno privilegiati rispetto a quelli di tipo punitivo-sanzionatorio: • rinforzo dei comportamenti corretti; • ridefinizione partecipata delle regole sociali di convivenza; • gestione positiva dei conflitti e moderazione dell'eccessiva competitività; • promozione di reti di solidarietà, • promozione della conoscenza e della gestione delle emozioni.

Personale scolastico		
• Navigazione su siti non necessari all'attività didattica per interessi privati e personali che esulano dalle attività scolastiche; • Alterazione dei parametri di protezione dei computer in uso; • Installazione di software o salvataggio di materiali non idonei; • Utilizzo delle comunicazioni elettroniche con i genitori e con gli alunni non compatibili con il ruolo professionale; • Trattamento dei dati personali, comuni e sensibili degli alunni non conforme alla normativa sulla privacy o che non garantiscano un'adeguata protezione degli stessi; • Diffusione delle password assegnate; • Custodia inadeguata degli strumenti digitali cui possono accedere terzi non autorizzati; • Inadeguata formazione preventiva degli alunni sull'utilizzo corretto e responsabile delle tecnologie digitali e di internet; • Vigilanza inadeguata degli	Nel caso di infrazione consapevole da parte dei docenti o del personale non docente, sarà compito del Dirigente Scolastico intervenire per via amministrativa secondo le norme vigenti. Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza (l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, l'utilizzo di piattaforme) e procedere alla rimozione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone copia per eventuali successive investigazioni. In caso di applicazione della regola che prevede il ritiro del cellulare o di altri dispositivi, i genitori sono tenuti a prelevare personalmente il cellulare a scuola in base ai tempi stabiliti dalla Dirigenza.	In quanto parte di una comunità educativa, tutto il personale scolastico è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso. Inoltre, in quanto parte di una comunità educativa, il personale deve porsi come modello di comportamento virtuoso, consapevole che le infrazioni alla e-Safety determinano conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni.

alunni che può creare le condizioni per un utilizzo non autorizzato delle TIC oltre a possibili incidenti; • Insufficienti interventi di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale nelle situazioni critiche di contrasto a terzi.		
Genitori		
Situazioni potenzialmente a rischio: • piena autonomia concessa ai minori nella navigazione sul web e nell'utilizzo dello smartphone. • posizione del computer in ambienti non visibili a tutti quando utilizzato dai minori • utilizzo del pc in comune con gli adulti con la possibilità che i minori possano accedere a materiali non idonei conservati in memoria.	I genitori degli alunni possono essere convocati a scuola per concordare misure educative rapportate alla tipologia dell'infrazione commessa oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.	In quanto educatori, i genitori non solo devono porsi come modelli di comportamento virtuoso, ma devono conoscere le conseguenze civili e penali determinate da un mancato intervento educativo culpa in educando e/o culpa in vigilando).

MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO

La e-Safety Policy si inserisce all'interno di altre politiche scolastiche, quali la politica di protezione dei minori, la politica anti-bullismo, la politica del benessere degli alunni a scuola.

La e-Safety Policy sarà riesaminata annualmente o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola. L'animatore digitale, la Commissione preposta, i team digitali procederanno alla modifica, alla revisione, alla implementazione della Policy sotto la supervisione del DS, previa condivisione e discussione con il personale scolastico.

INTEGRAZIONE DELLA POLICY CON I REGOLAMENTI ESISTENTI

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti, che specificano il contesto di attuazione delle politiche dell'Istituto Comprensivo per un uso efficace e consapevole del digitale nella didattica:

- Patto di Corresponsabilità;
- PTOF, incluso il piano per l'attuazione del PNSD;
- POF;
- RAV;
- Regolamento interno d'istituto;
- Regolamento per la sicurezza informatica;
- Carta dei diritti e doveri della cittadinanza digitale.

FORMAZIONE E CURRICOLO

La Commissione preposta decide di fare riferimento alla proposta di curricolo verticale stilata dal DIRIGENTE TECNICO MIUR – USR VENETO, Franca Da Re.

COMPETENZA DIGITALE

DISCIPLINE DI RIFERIMENTO: tutte
DISCIPLINE CONCORRENTI: tutte

La competenza digitale è ritenuta dall'Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d'oggi. L'approccio per discipline scelto dalle Indicazioni non consente di declinarla con le stesse modalità con cui si possono declinare le competenze chiave nelle quali trovano riferimento le discipline formalizzate. Si ritrovano abilità e conoscenze che fanno capo alla competenza digitale in tutte le discipline e tutte concorrono a costruirla. Competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.

SEZIONE A: Traguardi formativi				
COMPETENZA CHIAVE EUROPEA:	**COMPETENZA DIGITALE**			
Fonti di legittimazione:	Raccomandazione del Parlamento Europeo e del Consiglio 18.12.2006 Indicazioni Nazionali per il Curricolo 2012			
	FINE CLASSE TERZA SCUOLA PRIMARIA		**FINE SCUOLA PRIMARIA**	
COMPETENZE SPECIFICHE	**ABILITA'**	**CONOSCENZE**	**ABILITA'**	**CONOSCENZE**
Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate	Utilizzare nelle funzioni principali televisore, video, telefono e telefonino Spiegare le funzioni principali e il funzionamento elementare degli apparecchi per la comunicazione e l'informazione Utilizzare il PC, con la supervisione dell'insegnante, per scrivere compilare tabelle; utilizzare alcune funzioni principali, come creare un file, caricare immagini, salvare il file. Individuare alcuni rischi fisici nell'uso di apparecchiature elettriche ed elettroniche e ipotizzare soluzioni preventive Individuare alcuni rischi nell'utilizzo della rete Internet e ipotizzare alcune semplici soluzioni preventive	I principali strumenti per l'informazione e la comunicazione: televisore, lettore video e CD/DVD, apparecchi telefonici fissi e mobili, PC Funzioni principali degli apparecchi per la comunicazione e l'informazione Funzionamento elementare dei principali apparecchi di informazione e comunicazione Rischi fisici nell'utilizzo di apparecchi elettrici ed elettronici Rischi nell'utilizzo della rete con PC e telefonini	Utilizzare consapevolmente le più comuni tecnologie, conoscendone i principi di base soprattutto in riferimento agli impianti domestici. Utilizzare semplici materiali digitali per l'apprendimento. Utilizzare il PC, alcune periferiche e programmi applicativi. Avviare alla conoscenza della Rete per scopi di informazione, comunicazione, ricerca e svago. Individuare rischi fisici nell'utilizzo delle apparecchiature elettriche ed elettroniche e i possibili comportamenti preventivi Individuare i rischi nell'utilizzo della rete Internet e individuare alcuni comportamenti preventivi e correttivi	Semplici applicazioni tecnologiche quotidiane e relative modalità di funzionamento I principali dispositivi informatici di input e output I principali software applicativi utili per lo studio, con particolare riferimento alla videoscrittura, alle presentazioni e ai giochi didattici. Semplici procedure di utilizzo di Internet per ottenere dati, fare ricerche, comunicare Rischi fisici nell'utilizzo di apparecchi elettrici ed elettronici Rischi nell'utilizzo della rete con PC e telefonini

SEZIONE A: Traguardi formativi		
COMPETENZA CHIAVE EUROPEA:	**COMPETENZA DIGITALE**	
Fonti di legittimazione:	Raccomandazione del Parlamento Europeo e del Consiglio 18.12.2006 Indicazioni Nazionali per il Curricolo 2012	
FINE SCUOLA SECONDARIA DI PRIMO GRADO		
COMPETENZE SPECIFICHE	**ABILITA'**	**CONOSCENZE**
Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate	Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti in diverse situazioni. Conoscere gli elementi basilari che compongono un computer e le relazioni essenziali fra di essi. Collegare le modalità di funzionamento dei dispositivi elettronici con le conoscenze scientifiche e tecniche acquisite. Utilizzare materiali digitali per l'apprendimento Utilizzare il PC, periferiche e programmi applicativi Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago Riconoscere potenzialità e rischi connessi all'uso delle tecnologie più comuni, anche informatiche	Le applicazioni tecnologiche quotidiane e le relative modalità di funzionamento I dispositivi informatici di input e output Il sistema operativo e i più comuni software applicativi, con particolare riferimento all'office automation e ai prodotti multimediali anche Open source Procedure per la produzione di testi, ipertesti, presentazioni e utilizzo dei fogli di calcolo Procedure di utilizzo di reti informatiche per ottenere dati, fare ricerche, comunicare Caratteristiche e potenzialità tecnologiche degli strumenti d'uso più comuni Procedure di utilizzo sicuro e legale di reti informatiche per ottenere dati e comunicare (motori di ricerca, sistemi di comunicazione mobile, email, chat, social network, protezione degli account, download, diritto d'autore, ecc.) Fonti di pericolo e procedure di sicurezza

SEZIONE B: Evidenze e compiti significativi	
COMPETENZA CHIAVE EUROPEA:	**COMPETENZA DIGITALE**
EVIDENZE	**COMPITI SIGNIFICATIVI**
Riconosce e denomina correttamente i principali dispositivi di comunicazione ed informazione (TV, telefonia fissa e mobile, Computer nei suoi diversi tipi, Hifi ecc.) Utilizza i mezzi di comunicazione che possiede in modo opportuno, rispettando le regole comuni definite e relative all'ambito in cui si trova ad operare È in grado di identificare quale mezzo di comunicazione/informazione è più utile usare rispetto ad un compito/scopo dato/indicato Conosce gli strumenti, le funzioni e la sintassi di base dei principali programmi di elaborazione di dati (anche Open Source).	**ESEMPI** Utilizzare i mezzi informatici per redigere i testi delle ricerche, delle relazioni, dei rapporti, degli esperimenti; Utilizzare fogli elettronici per effettuare calcoli, misure, statistiche, rappresentare e organizzare i dati; Utilizzare power point per effettuare semplici presentazioni Costruire semplici ipertesti Utilizzare la posta elettronica per corrispondere tra pari, con istituzioni, per relazionarsi con altre scuole anche straniere; applicare le più comuni misure di sicurezza anti-spam, anti-phishing Utilizzare Internet e i motori di ricerca per ricercare informazioni, con la supervisione dell'insegnante e utilizzando le più semplici misure di sicurezza per prevenire crimini, frodi e per tutelare la sicurezza dei dati e la riservatezza Rielaborare un breve testo che pubblicizzi il sito della scuola Rielaborare una presentazione della scuola Rielaborare un file per il calcolo delle spese e delle entrate personali

Produce elaborati (di complessità diversa) rispettando una mappa predefinita/dei criteri predefiniti, utilizzando i programmi, la struttura e le modalità operative più adatte al raggiungimento dell'obiettivo.	Rielaborare i dati di una rilevazione statistica effettuata all'interno della scuola (predisponendo tabelle e grafici), e rendendola pubblica. Rielaborare una brossure sui pericoli dei mezzi di comunicazione informatici da divulgare ai compagni più piccoli Elaborare ipertesti tematici

SEZIONE C: Livelli di padronanza				
COMPETENZA CHIAVE EUROPEA:	**COMPETENZA DIGITALE**			
LIVELLI DI PADRONANZA				
1	**2**	**3**	**4**	**5**
Sotto la diretta supervisione dell'insegnante identifica, denomina e conosce le funzioni fondamentali di base dello strumento; con la supervisione dell'insegnante, utilizza i principali componenti, in particolare la tastiera. Comprende e produce semplici frasi associandole a immagini date.	Sotto la diretta supervisione dell'insegnante e con sue istruzioni, scrive un semplice testo al computer e lo salva. Comprende semplici testi inviati da altri via mail; con l'aiuto dell'insegnante, trasmette semplici messaggi di posta elettronica. Utilizza la rete solo con la diretta supervisione dell'adulto per cercare informazioni	Scrive, revisiona e archivia in modo autonomo testi scritti con il calcolatore. Costruisce tabelle di dati con la supervisione dell'insegnane; utilizza fogli elettronici per semplici elaborazioni di dati e calcoli, con istruzioni. Confeziona e invia autonomamente messaggi di posta elettronica rispettando le principali regole della netiquette. Accede alla rete con la supervisione dell'insegnante per ricavare informazioni Conosce e descrive alcuni rischi della navigazione in rete e dell'uso del telefonino e adotta i comportamenti preventivi	Scrive, revisiona e archivia in modo autonomo testi scritti con il calcolatore; è in grado di manipolarli, inserendo immagini, disegni, anche acquisiti con lo scanner, tabelle. Costruisce tabelle di dati; utilizza fogli elettronici per semplici elaborazioni di dati e calcoli Utilizza la posta elettronica e accede alla rete con la supervisione dell'insegnante per ricavare informazioni e per collocarne di proprie. Conosce e descrive i rischi della navigazione in rete e dell'uso del telefonino e adotta i comportamenti preventivi	Utilizza in autonomia programmi di videoscrittura, fogli di calcolo, presentazioni per elaborare testi, comunicare, eseguire compiti e risolvere problemi. Sa utilizzare la rete per reperire informazioni, con la supervisione dell'insegnante; organizza le informazioni in file, schemi, tabelle, grafici; collega file differenti. Confronta le informazioni reperite in rete anche con altre fonti documentali, testimoniali, bibliografiche. Comunica autonomamente attraverso la posta elettronica. Rispetta le regole della netiquette nella navigazione in rete e sa riconoscere i principali pericoli della rete (spam, falsi messaggi di posta, richieste di dati personali, ecc.), contenuti pericolosi o fraudolenti, evitandoli.

Livello 3: atteso a partire dalla fine della scuola primaria
Livello 4: atteso nella scuola secondaria di primo grado
Livello 5: atteso alla fine della scuola secondaria di primo grado

FORMAZIONE DEI DOCENTI SULL'UTILIZZO E L'INTEGRAZIONE DELLE TIC NELLA DIDATTICA E SULL'UTILIZZO CONSAPEVOLE, SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI

Al fine di favorire il continuo aggiornamento sui temi delle tecnologie digitali, sia in termini di utilizzo ed integrazione delle TIC nella didattica, sia di utilizzo consapevole e sicuro di Internet e delle tecnologie digitali, verranno promosse iniziative volte al confronto ed allo scambio di idee e di pratiche innovative:

- ✓ attività formative interne (seminari, workshop, attività laboratoriali…), avvalendosi di risorse interne e/o esterne;
- ✓ diffusione di informazioni circa opportunità formative esterne in presenza e/o a distanza anche nell'ambito del PNSD;
- ✓ bacheche on line per la condivisione di materiali per l'aggiornamento sull'uso delle TIC, fruibili accedendo al sito della scuola:
  - Progetto "Programma il futuro": Pensiero computazionale; attività di pensiero computazionale.
  - "Progetto Generazioni connesse", un percorso guidato che consente di riflettere sul proprio approccio alle tematiche legate alla sicurezza online e all'integrazione delle tecnologie digitali nella didattica. Il progetto si inserisce nel quadro delle attività svolte dal Ministero dell'Istruzione, dell'Università e della Ricerca per dare attuazione all' art 1, comma 7, lettera l della legge 107 del 13 luglio 2015 - "la Buona Scuola", e alle azioni contenuti nel Piano Nazionale per la prevenzione del bullismo e del cyberbullismo a scuola.
- ✓ Canale Istituto "Griffini" – Piattaforma "Youtube" per la visione di tutorial sull'uso delle TIC e sull'uso del registro elettronico.
- ✓ Registro elettronico-Sezione Skoodle-corso Condivisione documenti per la fruizione di documenti, materiali, sitografia e risorse multimediali sul fenomeno del Cyberbullismo.

SENSIBILIZZAZIONE DELLE FAMIGLIE

Per valorizzare la sinergia degli interventi educativi di scuola e famiglia, garanzia per il successo scolastico ed educativo di ogni studente, le indicazioni della e-Safety diventano parte integrante del Patto Educativo di Corresponsabilità stipulato con le famiglie degli alunni.

Verranno inoltre valorizzate le opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità o che coinvolgono la Rete del Progetto "Ondamedia" (AVIS, Donne in Circolo, Ente comunale e Servizi, Polisportiva iuventina, Polizia Postale, Tribunale di Lodi, Arma dei Carabinieri, Telefono Azzurro…).

GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA

ACCESSO AD INTERNET: FILTRI ANTIVIRUS E SULLA NAVIGAZIONE

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

Le postazioni sono dotate di software antivirus, con assistenza tecnica da remoto o in sede.

I docenti e tutta la comunità scolastica vengono sensibilizzati sull'opportunità di mantenere aggiornati gli antivirus installati sulle macchine personali e controllare i dispositivi di archiviazione esterna che vengano collegati ai pc della scuola. In caso di virus particolarmente pericolosi, vengono inviate informazioni digitali e/o cartacee.

Nei laboratori destinati agli allievi si stanno rigenerando i pc dei primi anni 2000 passando da Win XP al sistema operativo di distribuzione GNU/Linux, allo scopo di recuperare i vecchi pc, ridurre al minimo i costi delle licenze acquistate dalla scuola, formare gli allievi all'uso di prodotti open source, fornire una maggiore protezione da infezioni di virus.

GESTIONE ACCESSI (PASSWORD, BACKUP, ECC.)

L'Istituto è dotato di una rete wireless in tutti i plessi.

La password è unica a livello di Istituto/plesso, ma la scuola sta valutando l'ipotesi di assegnare una password per ciascun utente allo scopo di monitorare meglio eventuali usi impropri e di estendere il servizio.

Ciascun utente connesso alla rete dovrà:

- rispettare il presente regolamento e la legislazione vigente succitata;
- tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso e rispettare la cosiddetta netiquette (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o e-mail);
- I genitori saranno invitati a firmare e restituire un modulo di consenso;
- La componente studentesca dovrà impegnarsi a rispettare le norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet.

E-MAIL

L'Istituto fornisce

- una casella di posta elettronica @iccasalpusterlengo.edu.it a tutto il personale docente e ATA;
- un unico account per accedere al registro on-line e a Skoodle ad ogni alunno e ai relativi genitori;

Sulla rete scolastica tutti sono invitati a utilizzare solo account di posta elettronica presenti nel dominio scolastico e per scopi inerenti lo svolgimento didattico/organizzativo.
Le comunicazioni tra personale scolastico, famiglie e allieve/allievi via e-mail devono avvenire preferibilmente tramite un indirizzo e-mail della scuola o all'interno della piattaforma di apprendimento, per consentire l'attivazione di protocolli di controllo.
e-mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti.

SITO WEB DELLA SCUOLA E BLOG

I contatti sul sito web sono: indirizzo della scuola, e-mail e numero di telefono.

Il sito prevede solo un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale, e un'area riservata accessibile solo dopo autenticazione.

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

Per quanto riguarda l'accessibilità e il rispetto della normativa in merito ai siti scolastici, il nostro Istituto si avvale della collaborazione con la ditta Kedea.

SOCIAL NETWORK

L'istituto comprensivo di Casalpusterlengo, consapevole della grande importanza rivestita dai social network nella vita quotidiana dei giovani di oggi, considera tale argomento punto focale del progetto.

A tal fine la Commissione preposta al Progetto "Ondamedia" pianificherà corsi di formazione per alunni, docenti e genitori sui temi della navigazione in sicurezza e della cittadinanza digitale.

Nelle lezioni si dovrà comunque sempre tenere presente che l'accesso alla rete nel suo complesso, visti anche i punti precedenti, ha assoluta necessità di una seppur minima competenza tecnica di base (che sarà pertanto oggetto di trattazione nelle lezioni).

Sarà compito della scuola educare i ragazzi ad un uso consapevole dei social network, in particolare sarà dato particolare rilievo a:

- privacy: quali foto-video possono essere postati,
- copyright (vietato postare contenuti protetti dal diritto d'autore),
- cyber-bullismo - adescamento on-line,
- commenti offensivi (netiquette).

REGISTRO ELETTRONICO

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni.

L'uso del registro elettronico è spiegato alle famiglie nel corso del primo consiglio di classe dell'anno scolastico e la pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante l'alunno/a.

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

PROTEZIONE DEI DATI PERSONALI

L'Istituto Comprensivo fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c. d. Codice della Privacy).

Si adotteranno strategie possibili per la protezione dei dati personali, particolarmente sensibili nel caso dei minori.

Gli alunni saranno istruiti nel prestare sempre molta attenzione a quali dati vengono messi on line (numeri di telefono, email, carte di credito, dati personali in genere…).

STRUMENTAZIONE PERSONALE

STUDENTI

Le indicazioni del MIUR sull'uso dei device a scuola: "Dieci punti per l'uso dei dispositivi mobili a scuola" (gennaio 2018) prevedono l'utilizzo per fini didattici dei dispositivi, tuttavia sanciscono l'autonomia decisionale di ogni singolo Istituto in merito al divieto d'uso.

In linea con le indicazioni del MIUR e come previsto dal Regolamento d'Istituto e dal Patto di Corresponsabilità, è vietato per tutti gli alunni dell'I.C portare a scuola qualsiasi tipologia di device (cellulari, tablet, macchine foto-video con connessione dati, lettori MP3, hard-disk portatili, ultra-book, net-book e altri dispositivi digitali di archiviazione dati). Il docente autorizzerà l'uso previa comunicazione al Dirigente scolastico, ai genitori attraverso un'informativa che preveda la firma della liberatoria sulle condizioni d'uso dei device.

Nello specifico, il telefono dei vari plessi deve essere usato per chiamate attinenti il servizio scolastico (comunicazioni con la Direzione, chiamate alle famiglie per indisposizione degli alunni, accordi per progetti didattici…). In caso di comunicazioni urgenti gli alunni, previa autorizzazione dei docenti, dovranno rivolgersi al personale scolastico che provvederà a chiamare le famiglie. I genitori stessi dovranno utilizzare la linea telefonica della scuola per comunicazioni urgenti.

In caso di violazione delle suddette disposizioni, sarà previsto il ritiro temporaneo dei dispositivi da parte del docente che rileva la violazione. Quest'ultimo dovrà tempestivamente informare la famiglia dell'accaduto (anche telefonicamente), annotare la violazione sul registro di classe e compilare una "Scheda per la rilevazione di violazione delle disposizioni sulla strumentazione

personale" (di seguito allegata e disponibile nell'area riservata del sito web istituzionale). Il dispositivo verrà depositato in Segreteria e consegnato ai genitori. Alla seconda infrazione la famiglia verrà convocata dal Dirigente Scolastico e/o dai docenti del C.d.C per un colloquio.

Con la condivisione della presente Policy, "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone" a seguito di violazioni citate nella presente Policy

DOCENTI

In linea con le indicazioni del MIUR, come previsto dal Regolamento d'Istituto e dal Patto di Corresponsabilità, durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, come il tablet, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili (il computer di classe), in special modo per l'utilizzo del registro elettronico. Previa autorizzazione della Dirigenza, durante il restante orario di servizio, l'uso del cellulare è consentito solo per comunicazioni personali che rivestano carattere di urgenza, mentre l'uso di altri dispositivi elettronici personali è permesso per attività funzionali all'insegnamento.

La responsabilità sulla conservazione e corretta gestione dei dispositivi è affidata unicamente al proprietario.

PERSONALE DELLA SCUOLA

Come previsto dal Regolamento d'Istituto e dal Patto di Corresponsabilità, tutto il personale scolastico non è autorizzato ad utilizzare devices personali laddove stia assolvendo ad un ruolo didattico e/o lavorativo. L'uso dei dispositivi è consentito solo per comunicazioni urgenti a condizione che esso non intralci il normale svolgimento delle attività scolastiche, né distragga dal corretto svolgimento delle proprie mansioni. In tal caso la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente al proprietario.

Nell'invitare tutta la comunità scolastica (studenti, docenti, personale e famiglie) ad evitare, per quanto non necessario, la pubblicazione in rete di immagini e/o video ripresi all'interno dell'Istituto (fatta salva la pubblicazione da parte dei docenti in relazione a scopi didattici e/o professionali, previa informativa al Dirigente Scolastico), è bene ricordare che, secondo la normativa vigente, non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese e che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone costituisce una violazione punibile con sanzioni disciplinari, pecuniarie e anche penali.

PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

PRINCIPI GENERALI

Durante la navigazione tra i servizi dei Social Network o l'interazione in una community, l'utente deve sapere che:

- ✓ saranno segnalati e rimossi contenuti impropri e/o illeciti, pur garantendo la libertà di espressione;

- ✓ è imprescindibile conoscere i diritti e i doveri (carta dei diritti di internet);
- ✓ condividere informazioni personali comporta scegliere con cura che cosa rendere pubblico e cosa rendere privato;
- ✓ è necessario proteggere la propria identità digitale con password complesse;
- ✓ è necessario chiedere il permesso di ciascun destinatario coinvolto prima di effettuare la pubblicazione di elementi multimediali o informazioni che riguardano più persone;
- ✓ è illegale pubblicare sui Social video girati di nascosto e dove sono presenti persone filmate senza il loro consenso;
- ✓ bisogna diffondere i principi della sicurezza in rete, fornendo spiegazioni sulle regole di navigazione in rete a chi involontariamente commette abusi o errori, pubblicando materiale illecito, non idoneo o offensivo;
- ✓ è possibile segnalare tramite i canali e gli strumenti offerti dal servizio dei Social, ogni abuso subito o rilevato nella navigazione, chiedendo la rimozione del contenuto sul sito prima di procedere alla denuncia presso le autorità competenti;
- ✓ la scuola è chiamata ad adottare misure atte a prevenire e contrastare ogni forma di violenza e di prevaricazione;
- ✓ la famiglia è chiamata a collaborare, non solo educando i propri figli, ma anche vigilando sui loro comportamenti;
- ✓ il Patto Educativo di Corresponsabilità è determinante nella diffusione di valori che educhino al rispetto della diversità, al senso della comunità e della responsabilità collettiva.

SEZIONE FINALE POLICY

PROTOCOLLO DI INTERVENTO PER I CASI DI BULLISMO E DI CYBERBULLISO

PROCEDURE OPERATIVE IN CASO DI VIOLAZIONE DELLE DISPOSIZIONI SULLA STRUMENTAZIONE PERSONALE: scheda 1

PROCEDURA OPERATIVA DI RILEVAZIONE E GESTIONE DEI CASI: scheda 2
allegato 1,2: rilevazione dei casi
allegato 3: scheda di segnalazione caso
allegato 4,5,6: schemi di interventi in classe

SCHEDA NUMERI TELEFONICI INTERVENTI ESPERTI DI COUNSELING E DELLA LEGALITÀ: allegato7

MODELLO SEMPLIFICATO PER LA SEGNALAZIONE/RECLAMO di CONTENUTI ILLECITI IN MATERIA DI CYBERBULLISMO

LIBERATORIA PUBBLICAZIONE CONTENUTI DIGITALI

CONSENSO INFORMATO UTILIZZO NUOVE TECNOLOGIE: docenti, genitori, studenti

COMUNICAZIONE AI DOCENTI RELATIVA ALLE VIOLAZIONI DEI DATI a cura del DPO, dottor Giancarlo Favero

UNIONE EUROPEA
FONDI STRUTTURALI EUROPEI
PON 2014-2020
MIUR
Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
Direzione Generale per interventi in materia di edilizia scolastica, per la gestione dei fondi strutturali per l'istruzione e per l'innovazione digitale
Ufficio IV
PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO (FSE-FESR)

M.I.U.R.

Istituto Comprensivo di Casalpusterlengo ad Indirizzo Musicale

Via Olimpo, 6 26841 CASALPUSTERLENGO (LO)

Codice Meccanografico LOIC80900D Codice Fiscale 90518620159 Codice Univoco Ufficio UFTH6W

Tel. 037781940 – 037784379 E-mail: loic80900d@istruzione.it PEC loic80900d@pec.istruzione.it www.iccasalpusterlengo.edu.it

INTRODUZIONE

Con il presente protocollo si intende offrire ai docenti un supporto operativo che aiuti a prevenire e ad affrontare le diverse situazioni legate ai fenomeni di bullismo e di cyberbullismo, come previsto dalla normativa esistente e in particolare dalla legge 29 maggio 2017, n. 71, recante **"**Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo**".**

Il protocollo è contenuto nella sezione finale della "Policy di Istituto" e nella sezione "Regolamenti di istituto", consultabile sul sito dell'I.C di Casalpusterlengo.

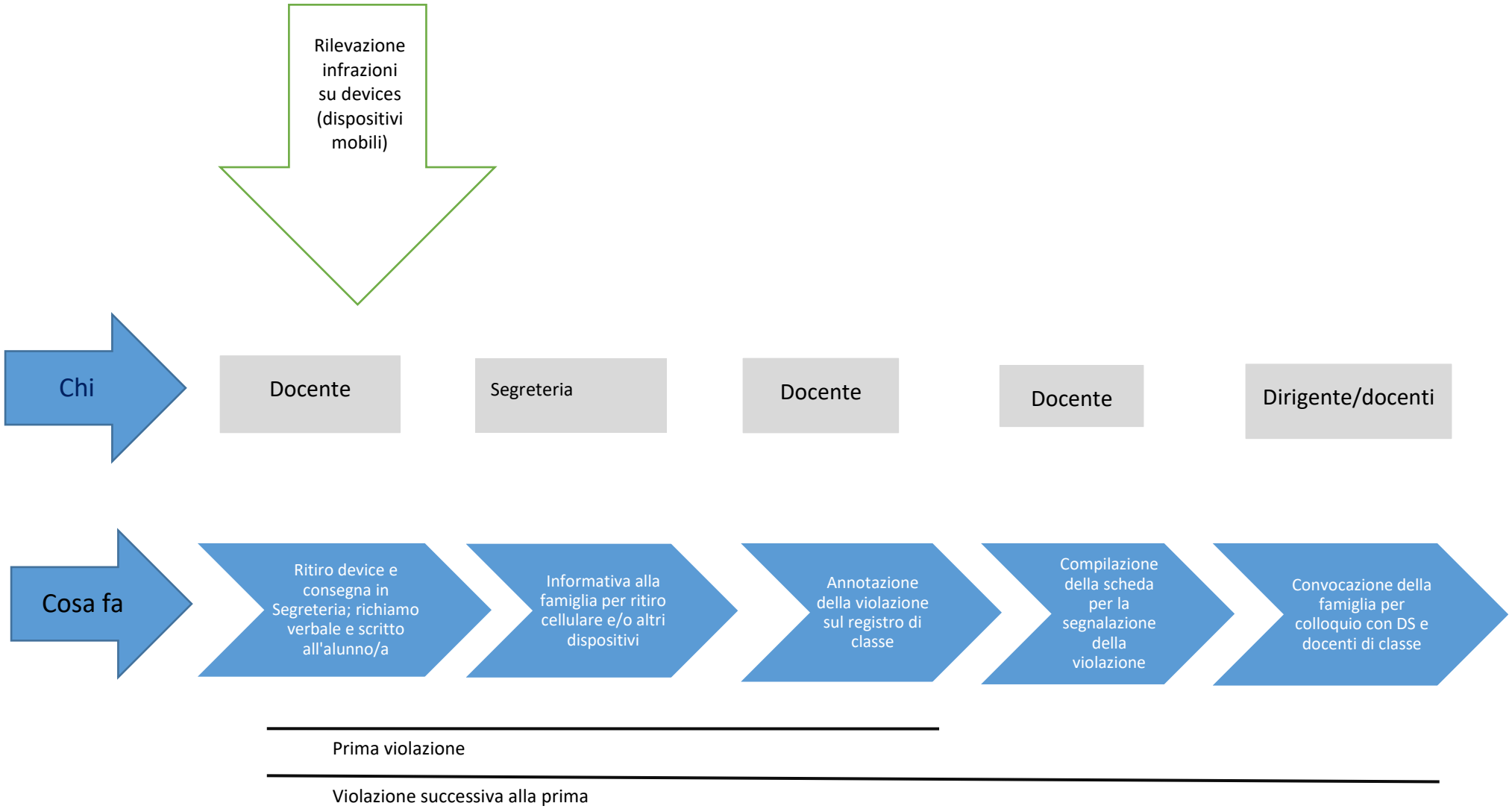
PREVENZIONE

Se ai docenti spetta il compito di essere promotori e garanti della costruzione dialogica di un percorso formativo partecipato, il loro ruolo diventa spesso inevitabilmente quello di confidenti degli alunni e delle loro esperienze. Proprio per questo, gli insegnanti sono chiamati a farsi carico delle problematiche e dei rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno. Basti pensare all'elevato numero di casi di bullismo e di cyberbullismo che gli insegnanti si trovano a gestire durante la prassi didattica quotidiana e che non possono e non devono sottovalutare, rivestendo essi il ruolo di pubblico ufficiale (art. 357 comma 1 c.p).
In elenco una esemplificazione di possibili rischi inerenti a situazioni che possono accadere in ambiente scolastico, in ambiente familiare o nel gruppo dei pari.

RISCHI	AZIONI
Discrasia tra rischio reale e rischio percepito durante la navigazione on line Accesso ad informazioni scorrette Possibile esposizione a contenuti violenti e non adatti all'età degli alunni Videogiochi diseducativi Pubblicità ingannevoli Virus informatici in grado di infettare computer e cellulari Possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e (adescamento) Rischio di molestie o maltrattamenti da coetanei (cyber-bullismo) Scambio di materiale a sfondo sessuale (sexting) Uso eccessivo di Internet/cellulare/videogiochi (dipendenza-ludopatia)…	Diffusione di un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web. Richiesta di volta in volta di un'autorizzazione esplicita da parte dei genitori all'utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro). Rispetto del divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli studenti in orario scolastico. Regolamentazione delle eventuali eccezioni (uso del cellulare per comunicazioni alunno-famiglia in occasione di uscite didattiche) sotto la supervisione diretta di un docente responsabile. Dotazione di dispositivi da parte della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list). Blocco dell'accesso a un sito o ad un insieme di pagine impedendone la consultazione. Controllo periodico di siti visitati dagli alunni/figli. Utilizzo di un software in grado di intercettare le richieste di collegamento e di respingere quelle non conformi alle regole stabilite dall'amministratore…

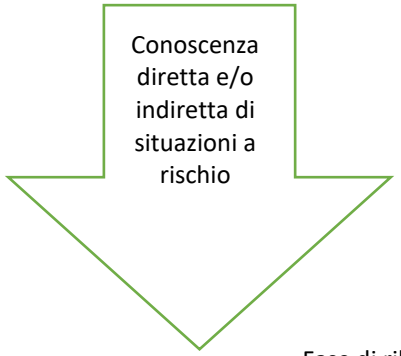
PROCEDURA OPERATIVA IN CASO DI VIOLAZIONE DEL REGOLAMENTO SULLA STRUMENTAZIONE PERSONALE: DISPOSITIVI MOBILI

scheda 1



PROCEDURA OPERATIVA DI RILEVAZIONE - GESTIONE DEI CASI DI CYBERBULLISMO E TABELLA SANZIONI

scheda2



Fase di rilevazione e di segnalazione

Fase di gestione dei casi

Chi

Docente	Docente	Docente/C.d.C.	Docente/i/Esperti/ Commissione	DS e Docenti	DS/docenti/famiglie	DS/docenti/famiglie

Cosa fa

All. 1,2 — All. 3 — All. 4,5,6 — All. 7

- Consultazione schede per la rilevazione dei casi
- Compilazione e consegna della scheda di segnalazione per informativa alla DS, alla Commissione e al C.d.C
- Annotazione della violazione sul registro di classe
- Interventi educativi in classe e osservazione feedback
- Convocazione della famiglia per colloquio con DS e docenti di classe
- Colloqui con esperti: pscicologo/a sportello ascolto
- Coinvolgimento attori esterni: polizia postale, guardia di finanza, carabinieri, questore servizi sociali

Rischi di lieve entità

Rischi di moderata entità

Rischi di elevata entità

Rischi di lieve entità	Sanzioni	Rischi di moderata entità	Sanzioni	Rischi di elevata entità	Sanzioni
<u>Studenti</u> ✓ Sottovalutare le netiquette condivise dalla classe e sottoscritte dall'intera comunità scolastica o dimostrare di non conoscere le regole del codice di condotta digitale (diritti e doveri della cittadinanza digitale) determinando comportamenti scorretti e al limite della legalità	• Richiamo orale da parte di una figura educativa • Richiamo scritto sul quaderno delle comunicazioni • Nota disciplinare sul registro di classe	✓ Disconoscere o misconoscere le netiquette (codice di condotta digitale) condivise dalla classe e sottoscritte dall'intera comunità scolastica determinando danni materiali alle strumentazioni e disagi psicologici e/o morali alle persone coinvolte	• Nota disciplinare sul registro di classe e sul quaderno delle comunicazioni • Risarcimento da parte della famiglia (genitori) del danno materiale causato dall'alunno/a • Colloquio dell'alunno/a e dei genitori con la psicologa/o dello sportello d'ascolto	✓ Trasgredire le regole della netiquette (codice di condotta digitale) condivise e sottoscritte dalla classe e/o dall'intera comunità scolastica determinando danni materiali irreversibili alle strumentazioni tecnologiche e danni psicologici e/o morali alle persone coinvolte	• Risarcimento da parte della famiglia del danno materiale • Denuncia e/o querela presso le autorità competenti di reati digitali da parte dell'istituzione scolastica previo accertamento della culpa in educando e in vigilando delle figure educative • Colloqui sistematici con la psicologa/o dello sportello d'ascolto • Sospensione dell'alunno/a
✓ <u>Docenti/Personale ATA</u>: Utilizzare i devices ad uso personale quando si sta assolvendo a un ruolo educativo e/o didattico ad eccezione di situazioni in cui le deroghe all'utilizzo sono autorizzate e concesse dal DS	• Richiamo orale del DS	✓ <u>Docenti:</u> utilizzare i devices ad uso personale nell'esercizio del proprio ruolo educativo e/o didattico determinando disagi, distrazione e interruzioni nello svolgimento delle attività scolastiche, salvo deroghe concesse e autorizzate dal DS	• Richiamo orale del DS	✓ Utilizzare i devices ad uso personale in modo tale che l'esercizio del proprio ruolo educativo e/o didattico sia compromesso, vilipeso o svilito o crei situazioni di illegalità.	• Notifica formale scritta della contestazione degli addebiti (entro 20 giorni dalla conoscenza della violazione) da parte del DS • Avvertimento scritto in caso di reiterazione della violazione • Censura e sospensione dal servizio sino a 10 giorni: provvedimento a carico dell'UST regionale

IN RELAZIONE ALLE TIPOLOGIE DI CYBERBULLISMO, OGNI CASO DOVRÀ ESSERE CONTESTUALIZZATO ED ANALIZZATO DAI DOCENTI E DAGLI ESPERTI PER INDIVIDUARE IL GRADO DI RISCHIO (LIEVE, MODERATO, ELEVATO) IN BASE AL QUALE COMMISURARE LE SANZIONI.	
CASI/TIPOLOGIE CYBERBULLISMO	**TIPOLOGIE SANZIONI DISCIPLINARI**
Flaming - Harassment - Denigration - Cyberstalking - Trichery o outing - Exclusion - Happy slapping - Sexting - Sextortion - Challenge autolesive - Hate speech - Adescamento on line	✓ Richiamo orale all'alunno/a da parte del docente e/o dei referenti della Commissione Ondamedia e/o del DS ✓ Richiamo scritto all'alunno/a e alla sua famiglia sul quaderno delle comunicazioni ✓ Nota disciplinare verbalizzata sul registro elettronico ✓ Lettera ufficiale di richiamo da parte del C.d. C ✓ Sospensione educativa anche attraverso l'esercizio di attività riparatorie o di utilità sociale ✓ Ammonimento delle autorità preposte (Questura, Polizia postale, Carabinieri) se non viene presentata querela e/o denuncia per i minori tra i 14 e i 18 anni, in materia di stalking (art. 612-bis c.p.), diffamazione (art. 595 c.p.), minaccia (art. 612 c.p.) e trattamento illecito di dati personali (art. 167 del codice della privacy) commessi mediante internet. * ✓ Querela e/o denuncia da parte dell'Istituzione scolastica per i minori tra i 14 e i 18 anni ✓ Sanzioni amministrative di tipo pecuniario commisurate all'entità del danno materiale, morale, biologico ed esistenziale ✓ Allontanamento dall'istituzione scolastica ✓ Sanzioni penali ed amministrative a carico della famiglia se dimostrata la culpa in vigilando e in educando (l'articolo 2048 del codice civile) ✓ Sanzioni penali ed amministrative a carico del personale docente se dimostrata la culpa in vigilando e in educando (articolo 2048 del codice civile) ✓ Sanzioni penali ed amministrative a carico del Dirigente scolastico se dimostrata la culpa in organizzando dell'Istituzione scolastica (ex articolo 2043 del codice civile) ✓ Risarcimento delle ore perse per ripristinare i danni al sistema informatico e per renderlo nuovamente operante ed affidabile. Rimangono comunque applicabili ulteriori sanzioni disciplinari, eventuali azioni civili per danni, nonché l'eventuale denuncia del reato all'Autorità Giudiziaria per il personale educativo e per i minori tra i 14 e i 18 anni ✓ Nel caso di infrazione consapevole da parte dei docenti o del personale non docente, sarà in ogni caso compito del Dirigente Scolastico intervenire per via amministrativa secondo le norme vigenti.

- Si puntualizza che il reato di ingiuria è stato depenalizzato, pertanto le sanzioni si configurano come civili e non più penali. Per approfondimenti: art. 594 c. p

ALLEGATO 1 TIPOLOGIE DI CYBERBULLISMO - GLOSSARIO

Flaming	Messaggi violenti e volgari mirati a suscitare una lite, un conflitto online.
Harassment	Dall'inglese "molestia": invio ripetuto di messaggi offensivi, scortesi ed insultanti.
Cyberstalking	Cyber-persecuzione: invio ripetuto di messaggi contenenti minacce o fortemente intimidatori.
Denigration	Denigrazione: invio o pubblicazione on line di pettegolezzi, dicerie crudeli o foto compromettenti per danneggiare la reputazione della vittima o le sue amicizie.
Impersonation	Sostituzione di persona: consiste nel violare l'account di qualcuno, nel farsi passare per questa persona inviando messaggi compromettenti per dare una cattiva immagine della stessa, crearle problemi o pericoli e danneggiarne la reputazione o le amicizie.
Outing and trickery	Rivelazioni e inganno: condivisione online di segreti o di informazioni imbarazzanti su un'altra persona. Lo scopo consiste nello spingere con l'inganno qualcuno a rivelare segreti o informazioni imbarazzanti e poi condividerle online.
Exclusion	Esclusione (bannare) deliberata di una persona da un gruppo online (come una lista di amici) per ferirla, isolarla e ghettizzarla.
Cyberbashing o happy slapping	Aggressioni violente che hanno inizio nella vita reale e poi continuano online attraverso l'uso di foto e video a scopo denigratorio e discriminatorio
Sextortion	Immissione su internet di messaggi e immagini sessualmente esplicite con finalità estorsive
Challenge autolesive	Forma di attacco al corpo per mostrare il proprio coraggio a se stessi e agli altri, in cui vince chi riesce a sopportare più a lungo il dolore, il tutto documentato e diffuso on line
Hate speech	Pubblicazione di contenuti a sfondo razzista o di incitamento all'odio sulle piattaforme digitali

Cyberbullismo: come riconoscerlo

Nella vita di bambini e adolescenti differenziare la vita reale da quella virtuale ha sempre meno senso. Le tecnologie digitali permeano la vita dei ragazzi i quali sempre più spesso sono connessi sia di giorno che di notte tramite smartphone e tablet. Anche la differenziazione tra bullismo e cyberbullismo (la sua componente online) ha senso solo in termini definitori. Per questo motivo questa sezione, pur trattando nello specifico la componente online del bullismo, fa riferimento al fenomeno nella sua interezza, perché solo uno sguardo ad ampio respiro su ciò che i ragazzi vivono e affrontano all'interno delle dinamiche tra pari può permettere agli adulti di essere per loro un valido supporto nella gestione e nel superamento di episodi di sopraffazione e violenza in tutte le forme in cui si possono esercitare, subire o osservare.

Bullismo e Cyberbullismo - differenze

Si definiscono **bullismo** tutte quelle situazioni caratterizzate da **volontarie** e **ripetute** aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Non si fa quindi riferimento ad un singolo atto, ma a una **serie di comportamenti** portati avanti ripetutamente nel tempo, all'interno di un gruppo, da parte di qualcuno che compie azioni o dice cose per avere potere su un'altra persona. Queste aggressioni spesso avvengono o iniziano negli **ambienti di aggregazione** dei ragazzi: da quello scolastico, a quello sportivo, a tutti gli altri ambienti in cui si ritrovano. Se si limitano alla quotidianità e alla vita offline dei ragazzi sono forme di bullismo.

Se però queste prevaricazioni si estendono anche alla vita online, si parla di **cyberbullismo**: il cyberbullismo è la forma online del bullismo. Si realizza attraverso l'invio di messaggi verbali, foto e/o video tramite cellulari, smartphones, pc, tablet (su social network, siti web, blog, Email, gruppi online, newsgroup, chat) ed ha gli stessi obiettivi della sua forma offline, ovvero quelli di insultare, offendere, minacciare, diffamare e/o ferire.

Caratteristiche del Cyberbullismo

L'impatto: la diffusione di materiale tramite internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online.)

La possibile anonimità: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile

L'assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio (la vittima può essere raggiungibile anche a casa)

L'assenza di limiti temporali: il cyberbullismo può avvenire a ogni ora del giorno e della notte.

L'assenza di empatia: non vedendo le reazioni della sua vittima alle sue aggressioni, il cyberbullo non è mai totalmente consapevole delle conseguenze delle proprie azioni e questo ostacola ancor di più la possibilità per lui di provare empatia - o rimorso a posteriori -, per ciò che ha fatto, se non viene aiutato ad esserne consapevole da un amico, da un insegnante o da altri.

Tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili delle azioni del cyberbullo facendo accrescere il suo potere; mettere un “like” su un social network, commentare o condividere una foto o un video che prende di mira qualcuno o semplicemente tacere pur sapendo, mette i ragazzi nella condizione di avere una responsabilità ancora maggiore.

Adescamento: come riconoscerlo

L’adescamento online, in inglese ***grooming***, è definibile come il tentativo da parte di un adulto di avvicinare un bambina/o o un adolescente per scopi sessuali, conquistandone la fiducia al fine di superare le resistenze emotive e instaurare con lui una relazione intima o sessualizzata.

Spesso tali adulti utilizzano la Rete come luogo ove adescare i minori, ove entrare in contatto con loro: i luoghi in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i Social Network, le app di instant messaging, i siti e le app di teen dating mentre la relazione sessuale può avvenire attraverso webcam o live streaming e portare anche a incontri dal vivo.

L’adescamento online è un processo manipolativo e pianificato, interattivo e fluido, controllante e controllato, facilitato dalla mole di informazioni di sé che bambine/i e ragazze/i condividono in Rete e che costituiscono importanti punti di partenza per agganciare la vittima.

Il fenomeno dell’adescamento online non conosce significative differenze di genere: sia i ragazzi che le ragazze, soprattutto se disorientati ed in una fase di costruzione della propria identità sessuale, possono risultare vulnerabili e più facili prede di adescatori. Come si è detto, è possibile descrivere un copione dell’adescamento, che consta di cinque principali fasi, la cui descrizione può essere utile ad agevolarne il riconoscimento.

-**Fase dell’amicizia iniziale**: l’adescatore effettua ripetuti contatti di socializzazione e conoscenza con la vittima individuata; una volta esplorato il contesto ed i suoi margini di libertà, avvia il processo volto a carpirne la fiducia, sintonizzandosi sui bisogni e sugli interessi di quel bambino o adolescente. Il passaggio a contenuti sempre più privati ed intimi è graduale: prima di passare a discorsi espliciti, l’adescatore condivide con il minore argomenti di interesse di quest’ultimo (es. hobbies, musica o giochi preferiti) ponendogli frequenti domande di interessamento ed attenzione.

-**La fase di risk-assessment**: in seguito ai primi contatti con il minore individuato, l’adescatore testa il livello di ***privacy*** nel quale si svolge l’interazione con il bambino o l’adolescente (es. uso esclusivo o promiscuo del dispositivo attraverso il quale il bambino o adolescente sta interagendo). L’adescatore, come vedremo a breve, punta gradualmente all’esclusività, isolando il minore e lavorando al fine di passare, ad esempio, da una chat pubblica ad una privata, da una chat alle conversazioni attraverso il telefono, per poterne carpire il numero.

-**Fase della costruzione del rapporto di fiducia**: le confidenze e le tematiche esplorate divengono via via più private ed intime o comunque molto personali. L’adescatore può iniziare a fare regali di vario tipo alla vittima; in questa fase, può avvenire lo scambio di immagini, subito non necessariamente a sfondo sessuale. È proprio in ragione della fiducia costruita nell’interazione che le vittime di adescamento riferiscono di sentirsi umiliate, usate, tradite e tendono a sentirsi in colpa e ad auto-svalutarsi per essere cadute nella trappola.

-**Fase dell’esclusività**: l’adescatore rende la relazione con il minore impenetrabile agli esterni, isolandolo dai suoi punti di riferimento anche grazie alla fondamentale dimensione del segreto. L’obiettivo dell’adescatore è ottenere e mantenere il silenzio della vittima, anche attraverso il ricatto e l’abuso psicologico, per rimanere impunito. La vittima viene indotta a fidarsi ciecamente dell’abusante che appare essere interessato, attento e premuroso.

-**Fase della relazione sessualizzata**: una volta certo del territorio sicuro costruito con minuziosa pazienza, la richiesta di immagini o video potrebbe essere più insistente o più esplicita, così come la richiesta di incontri offline. L'adescatore normalizza la situazione al fine di vincere le eventuali resistenze del minore a coinvolgersi in tale rapporto.

Qualora un adulto dovesse sospettare o avere certezza rispetto alla possibilità che un minore sia coinvolto o si stia coinvolgendo in una situazione di questo tipo, è importante che non si sostituisca al minore stesso, ad esempio nel rispondere all'adescatore.

È fondamentale che venga tenuta traccia degli scambi intercorsi (es. salvare le conversazioni, fare degli screenshots) **rivolgendosi il prima possibile alla Polizia Postale e delle Comunicazioni.**

In seguito alla tempestiva gestione degli aspetti strettamente inerenti la Rete e la denuncia, è altresì importante valutare la possibilità di rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di **fornire al minore anche un adeguato supporto di tipo psicologico**. Spesso, infatti, i ragazzi riferiscono, da un lato, di sentirsi traditi e dall'altro, di sentirsi in colpa per aver riposto la propria fiducia in un soggetto il cui intento era negativo ed il cui interesse espresso non era reale.

Sexting: come riconoscerlo

Il *sexting* (crasi dei termini inglesi *sex* e texting) rappresenta la pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale (MMS), come foto di nudo o semi-nudo, via cellulare o tramite Internet (Levick & Moon 2010). Oggi si usano Whatsapp, Snapchat e app simili, ma i risultati sono gli stessi, se non, a causa della maggiore facilità e gratuità, ancora più gravi.

Un esempio pratico sono quelle situazioni in cui gli adolescenti producono, condividono e diffondono immagini "sexy" di se stessi o di coetanei, spesso fidanzati/e, utilizzando le webcam dei PC o, più spesso, le fotocamere integrate agli smartphone.

Le dinamiche di *sexting* si contraddistinguono per alcune caratteristiche ricorrenti; le seguenti:

- **la fiducia tradita**: nella maggior parte dei casi, chi produce ed invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo inoltre alla motivazione originaria della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);

- **la pervasività di diffusione dei contenuti**: in pochi secondi ed attraverso un solo click un contenuto può essere condiviso o diffuso ad un numero esponenziale di persone e piattaforme differenti; la diffusione può facilmente e velocemente divenire "virale";

-**la persistenza del fenomeno**: il materiale pubblicato in Rete vi può permanere anche per molto tempo e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

SCHEDA DI SEGNALAZIONE CASO

ALUNNO:			
CLASSE:		**SEZIONE:**	
PLESSO:		**ORDINE DI SCUOLA:**	

INFORMAZIONI relative a EPISODI PREGRESSI di Cyber-Bullismo, Sexting, Adescamento:	
RAPPORTI CON LA FAMIGLIA: (facoltativo)	
PROBLEMI socio relazionali EVIDENZIATI (facoltativo)	

OSSERVAZIONE DIRETTA	***EVENTO RIFERITO***	***TIPOLOGIA CASO***
☐	☐	Esposizione a contenuti violenti
☐	☐	Uso di videogiochi diseducativi
☐	☐	Accesso ed utilizzo di informazioni scorrette o pericolose
☐	☐	Scoperta ed utilizzo di virus in grado di infettare computer
☐	☐	Possibile adescamento
☐	☐	Cyberbullismo (rischio di molestie o maltrattamenti da coetanei…)
☐	☐	Sexting (scambio di materiale a sfondo sessuale)
☐	☐	Dipendenza da uso eccessivo (Social, videogiochi…)
☐	☐	Pubblicazione on line di contenuti lesivi della dignità e della reputazione altrui
☐	☐	Altro:
☐	☐	Altro

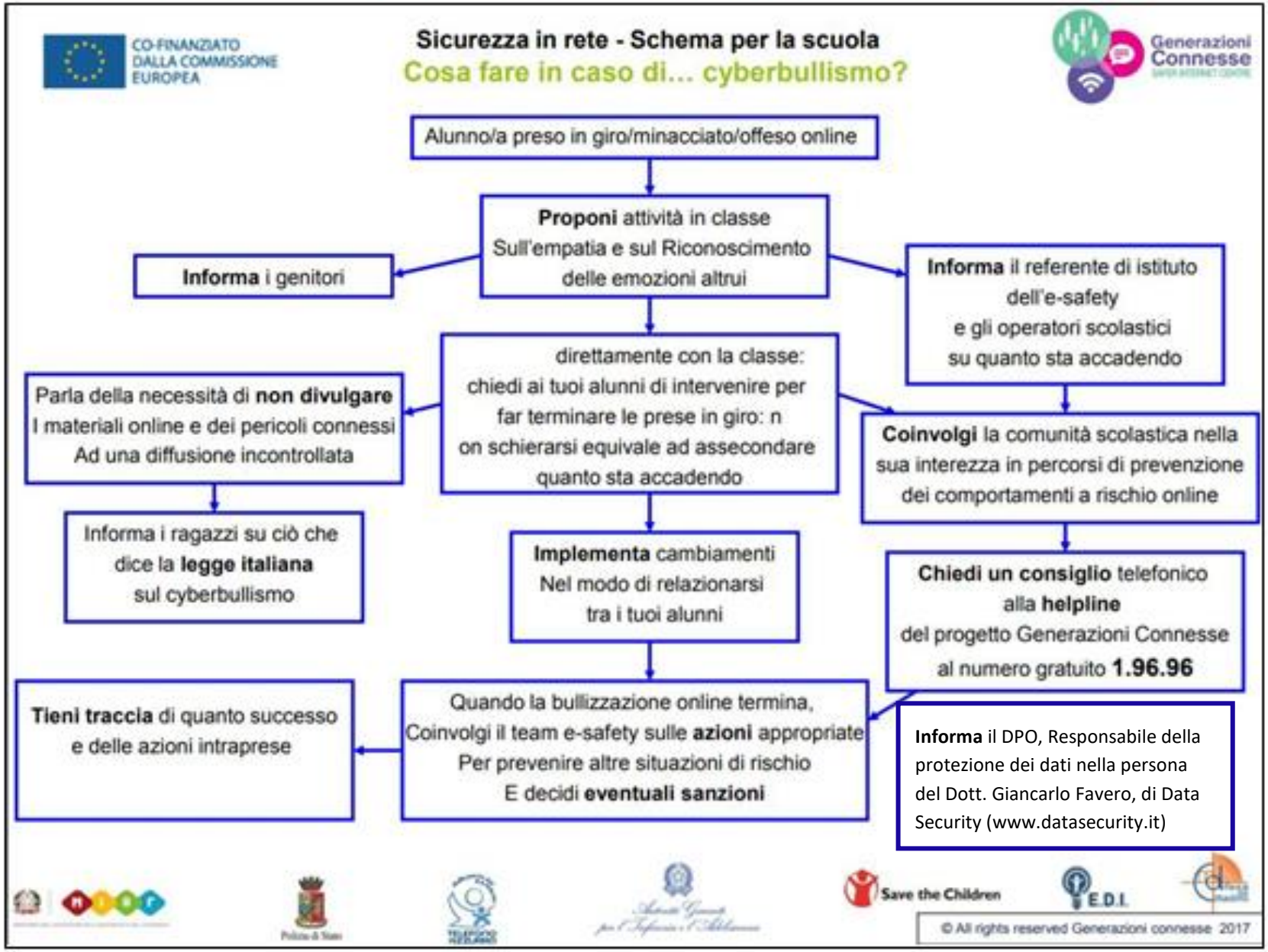
DESCRIZIONE del Caso: sintesi:	

Firma Docente/i coinvolti	----------	----------
	----------	----------

ALLEGATO 4

SCHEMA DI INTERVENTO : CYBERBULLISMO

IL Dirigente scolastico, previamente informato, concorda con il docente come procedere



ALLEGATO 5

SCHEMA DI INTERVENTO SEXTING

IL Dirigente scolastico, previamente informato, concorda con il docente come procedere

ALLEGATO 6

SCHEMA DI INTERVENTO: ADESCAMENTO

IL Dirigente scolastico, previamente informato, concorda con il docente come procedere

ALLEGATO 7 HELPLINE: INTERVENTO OPERATORI ESTERNI

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. Il servizio accoglie qualsiasi richiesta di ascolto e di aiuto da parte di bambini/e e ragazzi/e fino ai 18 anni o di adulti che intendono confrontarsi su situazioni di disagio/pericolo in cui si trova un minorenne. Il servizio di helpline è riservato, gratuito e sicuro, dedicato ai giovani o ai loro familiari che possono chattare, inviare Email o parlare al telefono con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza online.

1. **La linea di ascolto 1.96.96 e la** chat **di Telefono Azzurro**

2. **La Helpline 1.96.96 è attiva 24 ore al giorno, 365 giorni all'anno; la chat dal lunedì al venerdì (8-22) e sabato/domenica (8-20)**

Entrambe forniscono un aiuto immediato e competente su questioni quali:

Uso sicuro di Internet e dei social network - Adescamento online/grooming – Pedo-pornografia - Cyberbullismo – Sexting - pornografia e sessualità online degli adolescenti - Gioco d'azzardo online - Violazione della Privacy - Furto di identità in rete - Esposizione a contenuti nocivi online - Dipendenza da Internet - Esposizione a siti violenti, razzisti, che invitano al suicidio o a comportamenti alimentari scorretti (pro-anoressia e pro-bulimia) - Dipendenza da shopping online - Videogiochi online non adatti ai ragazzi.

URL SITO: http://www.azzurro.it/sostegno

1. **STOP-IT" di Save the Children**, un servizio che permette di segnalare la presenza di materiale pedopornografico online
2. Le segnalazioni raccolte da Stop-It, sono inviate al Centro Nazionale per il Contrasto della Pedo-pornografia su Internet (C.N.C.P.O.), istituito presso il servizio di Polizia Postale e delle Comunicazioni, seguendo procedure concordate e nel rispetto della privacy del segnalante, come disposto dalla legge in materia.
3. URL SITO: http://www.stop-it.it/

1. **Polizia postale:** la polizia delle comunicazioni è presente su tutto il territorio nazionale attraverso i 20 compartimenti, con competenza regionale, e le 80 sezioni con competenza provinciale, coordinati a livello centrale dal Servizio Polizia delle Comunicazioni.
Gli uffici sono dotati di indirizzi Email ai quali è possibile chiedere informazioni o inviare segnalazioni di violazione di norme penali nei settori della specialità:

URL SITO: http://www.commissariatodips.it/

Compartimento **Milano** Via Moisè Loria, 74 – tel. 02/43333011

Modello semplificato

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

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

INVIARE A

Garante per la protezione dei dati personali
indirizzo Email: cyberbullismo@gpdp.it

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

CHI EFFETTUA LA SEGNALAZIONE?

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

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

	<u>Chi è il minore vittima di cyberbullismo?</u> Nome e cognome Luogo e data di nascita Residente a Via/piazza

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

(indicare una o più opzioni nella lista che segue)

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

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

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

_____
_____
_____
_____
_____
_____

DOVE SONO STATI DIFFUSI I CONTENUTI OFFENSIVI?

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

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

1) _____
2) _____
3) _____

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

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

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

- ☐ Si, presso _____;
- ☐ No

Luogo, data

Nome e cognome

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

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

LIBERATORIA PUBBLICAZIONE ELABORATI DIGITALI

Dichiarazione liberatoria per la pubblicazione di elaborati, nomi, voci, immagini, materiale audiovisivo DIGITALE per iniziative esterne **all'Istituto Comprensivo di Casalpusterlengo**

Resa dai genitori degli alunni minorenni

Validità 1 anno

(D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" e adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679 in D.Lgs. 176 del 23/5/2018)

Io sottoscritto _____ , nato a _____ (____),

il _____ / _____ / _____ , residente a _____ (____) ,

indirizzo: _____ ;

Io sottoscritta _____ , nata a _____(___),

il _____ / _____ / _____ , residente a _____ (____) ,

genitori/e dell'alunno/a _____ frequentante la classe ___ sez. ___

( ) AUTORIZZANO

( ) NON AUTORIZZANO

la scuola a riprendere e/o a far riprendere in video e/o fotografare il/la propri__ figli__, in occasione di viaggi, visite d'istruzione e partecipazione ad eventi connessi all'attività didattica da sol__, con i compagni, con insegnanti e operatori scolastici, ai fini di:

- ✓ formazione, ricerca e documentazione dell'attività didattica (elaborati collocati all'esterno della scuola o in occasione di esposizioni, mostre…);
- ✓ divulgazione della ricerca didattica e delle esperienze effettuate sotto forma di documento in ambiti di studio (ad es. su DVD, sul sito web della scuola o su altri siti autorizzati…);
- ✓ stampe e giornalini scolastici;
- ✓ partecipazione a iniziative di sensibilizzazione alle problematiche sociali.

I genitori dichiarano di non aver nulla a pretendere in ragione di quanto sopra indicato e di rinunciare irrevocabilmente ad ogni diritto, azione o pretesa derivante da quanto sopra autorizzato.

Data_____

I genitori dell'alunno

(firma di entrambi i genitori)

_____ _____

CONSENSO GENITORI PER UTILIZZO CONSAPEVOLE INTERNET

Assunzione di responsabilità da parte dei GENITORI

I sottoscritti ……, e ……

genitori dell'alunno/a …… ……..

classe……sez……

dichiarano:

- di aver letto e compreso il Documento di e-Safety Policy;

- di essere al corrente che la Scuola mette in atto tutte le precauzioni necessarie per garantire che gli alunni usino correttamente la rete e non accedano a materiale inadeguato;

- di essere consapevoli che, in considerazione delle precauzioni prese per ridurre i rischi della navigazione sul WEB, la Scuola non è responsabile di eventuali usi impropri della rete e delle Tecnologie dell'Informazione e della Comunicazione (TIC) né della natura e dei contenuti del materiale che il/la proprio/a figlio/a, aggirando per volontà propria le barriere predisposte dalla scuola, potrebbero reperire in Internet;

- di essere consapevoli della responsabilità individuale del/la proprio/a figlio/a per le eventuali violazioni delle norme e/o per gli eventuali danni provocati da un uso improprio degli strumenti informatici;

- di essere consapevoli che, qualora non venissero rispettate le regole del codice di cittadinanza digitale, la scuola adotterà sanzioni disciplinari rapportate alla gravità degli episodi e saranno altresì possibili azioni civili e penali per eventuali danni, nonché l'eventuale denuncia all'autorità giudiziaria qualora la violazione si configuri come reato.

Firma del GENITORE

……

Firma del GENITORE

……

Data, ……

SCUOLA SECONDARIA DI I GRADO

CONSENSO STUDENTI PER UTILIZZO CONSAPEVOLE INTERNET

Assunzione di responsabilità da parte degli Studenti per l'uso consapevole di internet

Il/La sottoscritto/a ……, alunno/a della Classe

……, Sez. …… della Scuola Secondaria di primo grado "Griffini"

dichiara:

- di aver letto e compreso - all'interno del Documento di e-Safety Policy- la sezione relativa alle responsabilità dello studente;

- di essere consapevole che, a seguito di violazione volontaria delle regole in esso contenute, la Scuola avrà il diritto di sospendere l'accesso ad Internet e di adottare le sanzioni disciplinari previste.

Pertanto, il/la sottoscritto/a si impegna a:

- utilizzare le Tecnologie dell'Informazione e della Comunicazione (TIC) e la navigazione in internet in modo responsabile, secondo le regole previste dal Documento di e-Safety Policy.

Firma

……

Casalpusterlengo, …….

CONSENSO DEI DOCENTI PER UTILIZZO CONSAPEVOLE INTERNET

Assunzione di responsabilità da parte di Docenti e altro Personale della Scuola

Il/La sottoscritto/a ……, dipendente dell'Istituto Comprensivo di Casalpusterlengo, in qualità di ……

dichiara:

- di aver letto e compreso il Documento di e-Safety Policy;

- di essere consapevole delle responsabilità connesse all'uso delle Tecnologie dell'Informazione e della Comunicazione (TIC) nella scuola.

Pertanto, il/la sottoscritto/a si impegna a:

- tenere riservate le credenziali di accesso al sistema (Wi-Fi e aule di informatica);

- modificare la password del registro elettronico all'atto del primo collegamento;

- modificare periodicamente la password del registro elettronico, con frequenza almeno trimestrale ed ogniqualvolta la password abbia perso la segretezza;

- segnalare tempestivamente eventuali perdite di riservatezza;

- leggere la "Comunicazione ai docenti relativa alle violazioni dei dati"

- segnalare tempestivamente al Dirigente Scolastico e al Responsabile della protezione dei dati (Dott. Giancarlo Favero, Email: dpo@datasecurity.it tel. 335-5950674) qualsiasi evento di tipo violazione dei dati;

- utilizzare i computer e gli accessi esclusivamente per attività inerenti al proprio servizio e al l'aggiornamento professionale;

- non installare programmi senza possedere la licenza o app non sicure.

- segnalare eventuali anomalie;

- vigilare sul corretto utilizzo degli strumenti informatici e della navigazione in rete da parte degli alunni.

Firma

……

Casalpusterlengo, …….

COMUNICAZIONE AI DOCENTI RELATIVA ALLE VIOLAZIONI DEI DATI

Con la presente circolare si comunica che dalla data del 25 maggio 2018 è entrato definitivamente in vigore in seno a tutti gli Stati appartenenti all'Unione Europea il

Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati), detto anche brevemente **GDPR**, da General Data Protection Regulation.

Trattandosi di Regolamento e non di Direttiva, il Regolamento è immediatamente esecutivo ed applicabile all'interno di ciascuno Stato, senza bisogno di alcun recepimento.

Tra le numerose e significative novità introdotte dal GDPR, vi è l'obbligo per tutte le Pubbliche Amministrazioni di designare, ai sensi dell'art. 37, una figura del tutto nuova, e cioè il **Responsabile della protezione dei dati**, detto anche **DPO**, da Data Protection Officer.

In ottemperanza a tale obbligo, l'Istituto ha provveduto a designare il Responsabile della protezione dei dati nella persona del **Dott. Giancarlo Favero**, di Data Security (www.datasecurity.it), divisione sicurezza della ditta Swisstech S.r.l.

Tutti gli interessati (docenti, genitori, alunni, fornitori etc.) possono contattare il DPO all'indirizzo dpo@datasecurity.it oppure al numero 335-5950674, per porre qualsiasi quesito relativo alla normativa in materia di sicurezza e protezione dei dati, o relativo all'esercizio dei numerosi nuovi diritti dell'interessato introdotti dal GDPR.

In ottemperanza a quanto previsto dall'art. 37 comma 7 del GDPR, i dati di contatto del DPO sono stati comunicati al Garante per la protezione dei dati personali e saranno resi pubblici sul sito web istituzionale dell'Ente.

Una seconda significativa novità introdotta dal GDPR è l'obbligo per tutti i soggetti, sia pubblici che privati, di notificare al Garante per la protezione dei dati personali, entro 72 ore, alcune tipologie di evento riconducibili alla fattispecie di "**violazione dei dati personali**".

È pertanto necessario che tutto il personale docente e non docente sappia precisamente che cosa è una violazione dei dati personali, e le varie forme attraverso le quali tale evento può accadere.

Il GDPR all'art. 4 punto 12, fornisce la seguente definizione di violazione dei dati personali:

"***la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati***".

Contrariamente a quanto si potrebbe pensare, pertanto, la definizione di "*violazione di dati personali*" contempla non solo le fattispecie in cui vi sia stato un accesso abusivo ai dati personali, ma anche il caso della distruzione o della perdita dei dati personali, eventi che si possono verificare con una certa frequenza, ad esempio a causa del guasto di un supporto di memorizzazione, di un virus informatico, di un non corretto svolgimento delle procedure di *backup*, etc. Oppure può riguardare la casistica di dati personali o sensibili comunicati o portati a conoscenza di soggetti, interni o esterni all'Istituto, non autorizzati o non titolati.

Tra le casistiche di violazione dei dati personali che si possono verificare possiamo citare le seguenti:

- smarrimento di una chiavetta USB contenente dati personali
- furto di PC o tablet contenenti dati personali
- violazione del Registro elettronico
- smarrimento o furto di verifiche degli alunni
- non custodire adeguatamente i dati vaccinali
- portare a conoscenza dati di un alunno al genitore per il quale sia stato emesso un Provvedimento da parte del Tribunale dei minori di revoca della potestà genitoriale
- soddisfare una richiesta di accesso agli atti, che comporti la violazione della privacy del c.d. "controinteressati"
- pubblicare dati personali eccedenti rispetto a quelli strettamente indispensabili per il raggiungimento delle finalità.

È importante inoltre ricordare che la violazione dei dati personali non riguarda solamente i dati in formato elettronico, ma può riguardare anche i dati in formato cartaceo; questa seconda casistica, anzi, è la più critica da gestire, in quanto se vi fosse la perdita o il furto di fascicoli cartacei contenenti dati personali, tale evenienza potrebbe essere molto difficile da rilevare.

Nel dettaglio, l'art. 33 del Regolamento UE 2016/679 prevede:

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il

numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo."

Inoltre, l'art. 34 del Regolamento UE 2016/679 prevede:

"1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c)detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta."

Si chiede, pertanto, di porre la massima attenzione nel monitorare e rilevare tempestivamente tutti gli eventi di tipo "*violazione dei dati personali*", **compresi gli eventi per i quali non vi sia la certezza ma anche solo un sospetto**, e comunicarli immediatamente al Dirigente Scolastico, il quale provvederà ad informare tempestivamente il DPO, che provvederà ad effettuare tutte le valutazioni del caso di concerto con il Dirigente Scolastico ed a predisporre, se ve ne siano i presupposti, la notificazione da effettuare entro 72 ore all'Autorità di Controllo nazionale (Garante per la protezione dei dati personali).

Si ricorda che la tardiva od omessa notificazione al Garante di un evento di tipo "violazione dei dati personali" è punita con la **sanzione amministrativa pecuniaria fino a 10.000.000,00 di Euro**, ai sensi dell'art. 83 comma 4 lettera a del Regolamento Europeo.

Il Dirigente Scolastico
Pasqualina Lucini Paioni
Firma autografa omessa ai sensi
dell'art. 3 del D. Lgs. n. 39/1993

SITOGRAFIA

Documenti istituzionali

http://www.istruzione.it/allegati/2015/2015_04_13_16_39_29.pdf (linee di indirizzo Miur 2015)

http://www.miur.gov.it/documents/20182/0/Linee+Guida+Bullismo+-+2017.pdf/4df7c320-e98f-4417-9c31-9100fd63e2be?version=1.0 (linee di indirizzo Miur 2017)

http://usr.istruzione.lombardia.gov.it/wp-content/uploads/2016/11/Linee-guida-Lombardia-documentocyberbullismo-1-1.pdf (Linee di indirizzo regione Lombardia)

www.gazzettaufficiale.it/eli/id/2017/06/3/17G00085/sg (testo di legge)

www.generazioniconnesse.it (sito del progetto)

http://www.istruzione.it/scuola_digitale/allegati/Materiali/pnsd-layout-30.10-WEB.pdf (Piano Nazionale scuola digitale)

http://www.educazionedigitale.net/wp-content/uploads/2018/01/Decalogo-device.pdf (Decalogo per l'uso dei dispositivi mobili a scuola)

https://archivio.pubblica.istruzione.it/normativa/2007/allegati/prot30_07.pdf (Linee di indirizzo utilizzo cellulari 2007)

Siti degli Istituti Comprensivi consultati

www.icpascoliforgione.it

www.icaltavilla.gov.it/

www.ictulliazevi.gov.it

www.icolgiatecomasco.gov.it/

www.icviatrionfale.gov.it

www.icvittorioveneto1daponte.gov.it

www.comprensivocassino1.gov.it