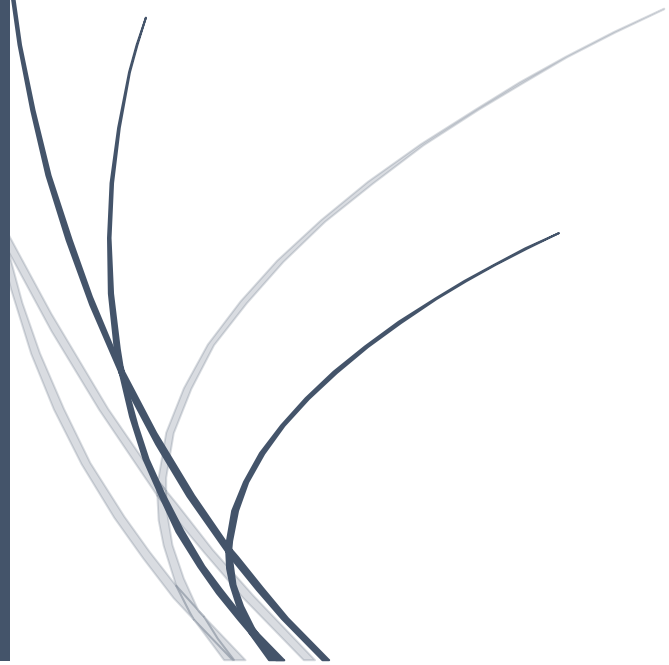
2018-2019

PROTOCOLLO DI INTERVENTO CASI DI CYBERBULLISMO

Istituto Comprensivo di Casalpusterlengo



Il dirigente scolastico

PASQUALINA LUCINI PAIONI

A cura della Commissione Ondamedia

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 EMail: 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**".**

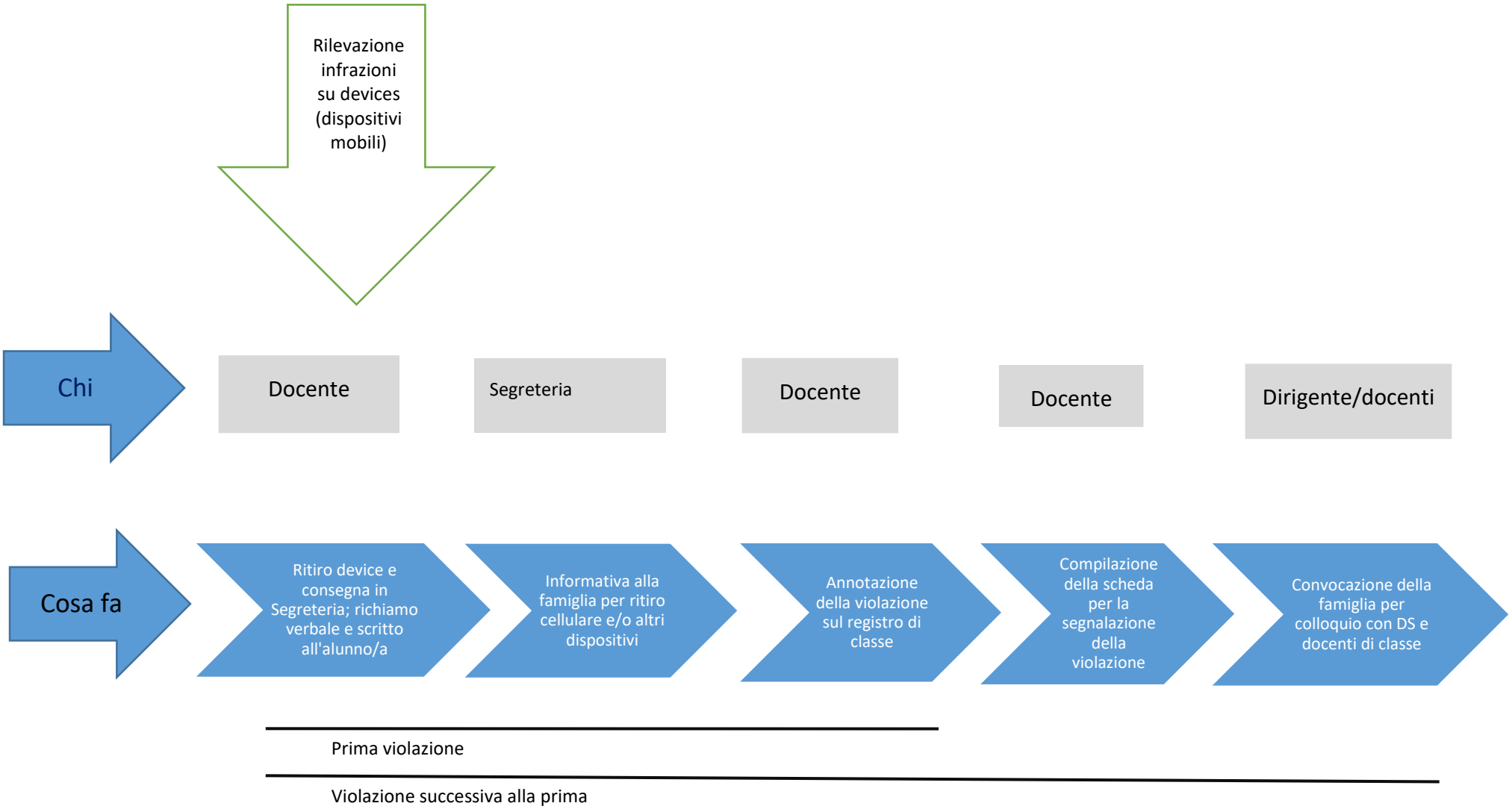
Il protocollo è contenuto nella sezione finale della "Policy di Istituto" e nella sezione "Regolamenti di istituto", consultabile sul sito dell'I.C di Casalpusterlengo.

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

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



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

Conoscenza diretta e/o indiretta di situazioni a rischio

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

CO-FINANZIATO DALLA COMMISSIONE EUROPEA

Sicurezza in rete - Schema per la scuola

Cosa fare in caso di… cyberbullismo?

Generazioni Connesse

Alunno/a preso in giro/minacciato/offeso online

Proponi attività in classe
Sull'empatia e sul Riconoscimento
delle emozioni altrui

Informa i genitori

Informa il referente di istituto
dell'e-safety
e gli operatori scolastici
su quanto sta accadendo

direttamente con la classe:
chiedi ai tuoi alunni di intervenire per
far terminare le prese in giro: n
on schierarsi equivale ad assecondare
quanto sta accadendo

Parla della necessità di **non divulgare**
I materiali online e dei pericoli connessi
Ad una diffusione incontrollata

Coinvolgi la comunità scolastica nella
sua interezza in percorsi di prevenzione
dei comportamenti a rischio online

Informa i ragazzi su ciò che
dice la **legge italiana**
sul cyberbullismo

Implementa cambiamenti
Nel modo di relazionarsi
tra i tuoi alunni

Chiedi un consiglio telefonico
alla **helpline**
del progetto Generazioni Connesse
al numero gratuito **1.96.96**

Tieni traccia di quanto successo
e delle azioni intraprese

Quando la bullizzazione online termina,
Coinvolgi il team e-safety sulle **azioni** appropriate
Per prevenire altre situazioni di rischio
E decidi **eventuali sanzioni**

Informa il DPO, Responsabile della protezione dei dati nella persona del Dott. Giancarlo Favero, di Data Security (www.datasecurity.it)

Save the Children

E.D.I.

ALLEGATO 5

SCHEMA DI INTERVENTO SEXTING

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

CO-FINANZIATO DALLA COMMISSIONE EUROPEA

Sicurezza in rete - Schema per la scuola

Cosa fare in caso di… sexting?

Generazioni Connesse

Alunno/a invia o riceve foto o video sessualmente espliciti

Se li ha ricevuti, spiega la legge sulla diffusione di materiale pedopornografico

Proponi attività in classe Sulla **fiducia e sull'affettività**

Se li ha inviati, spiega che contenuti condivisi online Possono rimanere o venire condivisi oltremodo,

Informa i genitori

Affronta direttamente con la classe: chiedi di non prendere in giro per quanto successo;

Informa il referente di istituto dell'e-safety. Se c'è wi-fii, sospendetelo.

Parla della necessità di **non divulgare** I materiali online e dei pericoli connessi Ad una diffusione incontrollata

Segnala ai servizi di Generazioni Connesse **"clicca e segnala"** o **"stop it"**.

Coinvolgi la comunità scolastica nella sua interezza in percorsi di prevenzione dei comportamenti a rischio online

Informa i ragazzi su ciò che dice la **legge italiana** Sulla diffusione di materiale pedopornografico

Implementa cambiamenti sulla modalità di condividere parti di sé - e una riflessione sulle relazioni - online

Chiedi un consiglio telefonico alla **helpline** del progetto Generazioni Connesse Al numero gratuito **1.96.96**

Informa il DPO, Responsabile della protezione dei dati nella persona del Dott. Giancarlo Favero, di Data Security (www.datasecurity.it)

Quando i contenuti sono rimossi/cancellati, coinvolgi il team e-safety sulle **azioni** appropriate **per prevenire** altre situazioni di rischio

Tieni traccia di quanto accaduto e delle azioni intraprese:

Polizia di Stato

Save the Children

E.D.I.

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 jn 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