



**Ministero dell'Istruzione, dell'Università e della Ricerca
I.I.S.S. GIUSEPPE GREGGIATI**

Via Roma, n.1 46035 Ostiglia (Mantova)

Tel. 0386/802360 -802301

email: mnis006003@istruzione.it

pec: mnis006003@pec.istruzione.it

sito istituzionale: www.giuseppereggiati.gov.it

C.F. 80024270201

Prot. Vedi segnatuta

Ostiglia, 28.04.2018

REGOLAMENTO E- SAFETY POLICY

INDICE

1. INTRODUZIONE

1.1. Premessa pag. 3

1.2. Scopo della Policy

1.3. Comunicazione e condivisione della Policy all'interno della comunità scolastica pag. 4

Condivisione e comunicazione della Policy agli alunni

Condivisione e comunicazione della Policy al personale

Condivisione e comunicazione della Policy ai genitori

1.4. Gestione delle infrazioni alla Policy pag. 5

Infrazioni degli alunni

Infrazioni del personale scolastico

1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento

1.6. Integrazione della Policy con regolamenti esistenti pag. 6

2. FORMAZIONE E CURRICOLO

2.1. Curricolo sulle competenze digitali per gli studenti pag. 6

2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica

e sull'uso consapevole di Internet e delle tecnologia digitali

2.3. Sensibilizzazione delle famiglie

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA

3.1. Accesso a internet pag. 7

3.2. Gestione accessi pag. 8

3.3. E-mail pag. 10

3.4. Blog e sito web della scuola

3.5. Social Network

3.6. Protezione dati personali

4. STRUMENTAZIONE PERSONALE

4.1. Studenti

4.2. Docenti pag. 11

4.3. Personale della scuola pag. 12

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.1. Prevenzione • Rischi • Azioni

5.2. Rilevazione • Cosa segnalare e come segnalare pag. 13

5.3. Gestione dei casi pag. 14

Definizione delle azioni da intraprendere a seconda della specificità dei casi pag. 15

Casi di cyberbullismo

Casi di sexting pag. 16

Casi di adescamento pag. 16

6. ANNESSI

6.1 Procedure operative per la gestione dei dati personali pag. 17

ALLEGATI

Modulo di segnalazione pag. 19

Diario di Bordo pag. 20

Black list firewall pag. 22

1. Introduzione

1.1. Premessa

Sia a livello internazionale, che nel contesto italiano, la presenza sempre più diffusa delle tecnologie digitali nella vita di tutti i giorni dei più giovani, compresi gli ambienti scolastici, apre nuove opportunità ma pone nuove attenzioni dal punto di vista del loro uso sicuro, consapevole e positivo. Inoltre, lo sviluppo e l'integrazione dell'uso delle TIC, ed in particolare di internet, nella didattica, offrono le condizioni e l'occasione per una trasformazione dell'insegnamento e dell'apprendimento nelle scuole e a tale proposito esistono numerose evidenze scientifiche sui benefici che l'uso delle tecnologie digitali possono apportare a tali aspetti. Ciò pone però delle sfide importanti, che riguardano più livelli di conoscenze, abilità e attitudini che i più giovani hanno bisogno di sviluppare, nell'ottica di accrescere le competenze digitali. Gli adulti hanno un ruolo fondamentale nel garantire che bambini/e e adolescenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro, ruolo che vede coinvolti a pieno titolo tutti coloro che hanno un ruolo educativo, oltre che formativo, in altre parole la comunità scolastica nel suo complesso, genitori inclusi. E' in questo quadro che si inserisce la necessità di affrontare la questione da più punti di vista e interessando più interlocutori, inclusi i più giovani, per arrivare a dotare ogni comunità scolastica di una propria Policy di E-safety.

1.2. Scopo della Policy

Con il termine Policy si intende un insieme di regolamenti, linee di azione e attività poste in essere per fare fronte ad una serie di necessità individuate. Una policy non è mai il risultato di un'azione unica, quanto piuttosto l'esito delle interazioni di un insieme di azioni e decisioni.

Il presente documento ha quindi lo scopo di descrivere:

- Le norme comportamentali e le procedure per l'utilizzo delle tecnologie digitali presenti in Istituto.
- Le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali. La nostra scuola ha prodotto un Piano d'Azione che individua il percorso e le risorse necessarie per elaborare e implementare una Policy di E-Safety, individuando due obiettivi principali:
- Adottare le misure atte a facilitare e a promuovere l'uso delle ICT nella didattica e negli ambienti scolastici;
- Stabilire le misure di prevenzione e di gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

1.3. Comunicazione e condivisione della Policy all'interno della comunità scolastica

Condivisione e comunicazione della Policy agli alunni:

- Nel corso dell'anno i docenti che nelle loro attività didattiche fanno uso delle TIC e in particolare modo dell'iPad dedicheranno alcuni momenti delle loro lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo.

Condivisione e comunicazione della Policy al personale:

- Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse negli organi collegiali (collegio docenti, riunioni di dipartimento) e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola.

Condivisione e comunicazione della Policy ai genitori:

- Le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento tramite pubblicazione sul sito.

1.4. Gestione delle infrazioni alla Policy

Infrazione degli alunni

Viene individuato come organo competente per la gestione delle infrazioni dei singoli alunni il Consiglio di Classe. I provvedimenti disciplinari da adottare nei confronti dell'alunno che ha commesso un'infrazione alla Policy, dopo aver tenuto conto sia dell'età dell'alunno che della gravità dell'infrazione commessa, saranno i seguenti: • richiamo verbale; • nota informativa sul diario ai genitori; • convocazione dei genitori per un colloquio con l'insegnante; • convocazione dei genitori per un colloquio con il Dirigente scolastico.

Infrazioni del personale scolastico

Le infrazioni alla Policy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole qui descritte sulla gestione della strumentazione, sia la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni. Nel primo caso la gravità si valuta sull'esposizione al rischio procurata agli alunni, nel secondo caso sul danno per la non tempestiva attivazione delle azioni qui indicate. La gestione delle infrazioni in quest'ambito ricade nella disciplina contrattuale.

1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento

Nel mese di maggio di ogni anno scolastico la commissione Bullismo e Cyberbullismo (formata da referente, animatore digitale, referente commissione PTOF, più un rappresentante per ogni plesso della scuola primaria e secondaria di primo grado) si riunirà con l'obiettivo di esaminare i casi problematici riscontrati durante l'anno e la loro gestione, in tale occasione valuterà la necessità o meno di modificare o implementare la Policy.

1.6. Integrazione della Policy con regolamenti esistenti

Il presente documento si integra pienamente per obiettivi e contenuti con il PTOF, incluso il piano per l'attuazione del PNSD e con i regolamenti già in vigore nell'Istituto quali: • Regolamento interno d'istituto; • Regolamento per l'utilizzo dei laboratori.

2. Formazione e curriculum

2.1. Curriculum sulle competenze digitali per gli studenti

Il curriculum sulle competenze digitali è in via di definizione, per ora si fa riferimento al modello nazionale della certificazione delle competenze.

2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'uso consapevole di Internet e delle tecnologia digitali

Le attività di formazione si svolgeranno su due livelli:

- Formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodi formativi;
- Formazione specifica di Istituto, legata alle esigenze formative rilevate ad inizio d'anno dal Collegio Docenti.

All'inizio di ogni anno scolastico la commissione Bullismo e Cyberbullismo, valutato a quali progetti/iniziative aderire e quali attività svolgere durante l'anno in corso, presenterà le sue proposte al Collegio Docenti per l'approvazione e la condivisione. Nel corso dell'anno scolastico 2017/2018, al fine di promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle ICT, e di prevenire e contrastare "ogni forma di discriminazione e di bullismo, anche informatico" (Legge 107/2015, art. 1, c. 7, l), il nostro Istituto aderirà al progetto **"Generazioni Connesse"** (SIC ITALY III), coordinato dal MIUR. Tale progetto prevede lo svolgimento di un Piano d'Azione che ha diversi ambiti di sviluppo, tra cui la formazione docente, ha inoltre aderito all'iniziativa del CORECOM, mettendo a

disposizione di alunni, docenti e genitori informazioni per un'eventuale procedura in caso di contenuti lesivi.

Per l'anno 2017/2018 la nostra scuola prevede di aderire ad iniziative proposte dagli organi competenti, partecipando a concorsi ed ad attività ,che verranno discusse nell'ambito della formazione regionale.

Il secondo percorso sarà a favore di quanti vorranno approfondire il tema del cyberbullismo in classe con il supporto di esperti e psicologi.

2.3 Sensibilizzazione delle Famiglie

Durante l'anno 2017/2018 il nostro Istituto richiederà l'intervento del CORECOM e della Polizia Postale per approfondire il tema della **Web Reputation** per sensibilizzare le famiglie sui rischi rappresentati dall'uso di cellulari, smartphone e chat-line senza un'adeguata formazione. Sarà creato sul sito della scuola un'area dedicata alla sicurezza in rete nella quale saranno inseriti materiali che illustrano i principali rischi che può incontrare un adolescente attraverso la navigazione in rete.

Tali materiali affronteranno tematiche quali il cyberbullismo, il sexting e l'adescamento. La scuola darà inoltre ampia diffusione, tramite pubblicazione sul sito, del presente documento di Policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e per favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola

3.1. Accesso ad Internet e 3.2. Gestione accessi (password)

L'accesso ad internet è possibile in tutti i plessi dell'Istituto

PLESSO DI OSTIGLIA

PREMESSA

La rete informatica in uso a Docenti e Studenti dell'Istituto G.Greggiati di Ostiglia verrà in questo documento definita "Rete Didattica", sia essa fruibile via cavo o Wi-Fi.

APPARATI DI RETE

Il controllo degli accessi, il monitoraggio ed il filtraggio dei contenuti nonché la conservazione dei log delle suddette attività viene gestita da un Firewall Stormshield SN-510. Gli accessi di amministrazione sono in possesso della dirigenza scolastica, del Preposto all'amministrazione di rete nominato dalla dirigenza scolastica e della ditta Carrara Computing International Srl.

L'utilizzo della rete Wi-Fi in uso presso l'istituto è gestito e monitorato da un controller Wi-Fi Ruckus Zone Director 1200.

ACCESSO ALLA RETE

L'accesso alla rete dell'istituto avviene tramite autentica basata su username e password nominali. Ciascuno studente e docente è in possesso delle proprie credenziali personali, necessarie per l'accesso alla rete. Inoltre, al fine di ispezionare il traffico SSL (HTTPS) in uscita ed ingresso, è necessario installare sugli apparati uno specifico certificato.

Tali procedure sono illustrate in appositi manuali in possesso del personale scolastico ed i link per l'accesso alle guide di utilizzo ed al materiale tecnico, come le password di accesso alla rete wifi pubblica, sono presenti sul sito dell'istituto.

SICUREZZA: URL FILTERING, SSL INSPECTION, APPLICATION PROTECTION

Al fine di garantire il rispetto dei dati sensibili, la protezione da attacchi di natura informatica ed al contempo impedire la fruizione di contenuti non ammissibili in ambito scolastico o vietati ai minori è stato implementato un enforcing della sicurezza basato sulle seguenti tecnologie:

- URL FILTERING

La Direzione Scolastica ha definito quali contenuti non rendere accessibili attraverso la rete scolastica (Es. gioco d'azzardo, pornografia). Queste categorie di siti web vengono rese inaccessibili attraverso un motore di url filtering aggiornato via cloud, il quale cataloga e discerne i siti visitati, bloccando i contenuti proibiti.

- **SSL INSPECTION**

Oltre al traffico in chiaro, anche tutte le connessioni criptate eseguite da e verso la rete dell'istituto vengono analizzate dal firewall per permettere allo stesso di bloccare contenuti pericolosi o vietati ed inibire l'uso di software dannosi od il collegamento a reti o servizi maliziosi o non sicuri.

- **APPLICATION PROTECTION**

Il firewall è in grado di discernere quali applicazioni sono in uso nei client agganciati alla rete d'istituto, per tanto è possibile inibire servizi illegali (Es. P2P) o applicazioni potenzialmente pericolose o inadatte all'ambito scolastico (Instant Messaging).

MONITORAGGIO & LOG

Qualsivoglia connessione, accesso o fruizione della rete informatica è tracciata e monitorata. Tutti i log delle attività e degli accessi vengono archiviati e sono a disposizione della dirigenza scolastica per la consultazione.

PRIVACY

I dati registrati riguardanti gli accessi ed il traffico, ed i relativi log sono anonimizzati. Qualsivoglia accesso a log contenenti dati sensibili o informazioni personali (accessi, utilizzo della rete, etc.) viene registrato e deve essere autorizzato dalla dirigente scolastica.

PLESSO DI POGGIO RUSCO

Per il plesso di Poggio Rusco si attiveranno le stesse strategie in atto ad Ostiglia. I lavori sono già stati appaltati e avranno inizio il 26.04.2018

3.3. E-mail

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Le credenziali sono in possesso del personale amministrativo. La posta elettronica è protetta da antivirus e da antispam.

3.4 Blog e sito web della scuola

Il sito istituzionale www.giuseppegreggiati.gov.it verrà dismesso entro la fine dell' a.s. 2017/18 e sostituito con un nuovo portale più attuale e aggiornato. L'accesso non prevede un **login in** per gli utenti non essendoci alcuna area riservata. Realizzato su CMS WordPress il nuovo sito www.istitutogreggiati.it sarà dotato di template responsive per garantire la massima fruibilità da tutti i dispositivi. Oltre a i collegamenti al registro elettronico, alla segreteria digitale e all'Albo Pretorio saranno presenti, con rispetto delle norme vigenti in materia, quelli ai social network (Facebook, Instagram, YouTube) che la scuola ha da poco implementato.

3.3 Social network

L'utilizzo dei social network nella didattica deve essere contestualizzato ad attività specifiche.

3.4 Protezione dei dati personali

Il trattamento dei dati personali riguarda unicamente le finalità istituzionali della scuola per le quali vengono raccolti solo i dati strettamente necessari. Essi saranno trattati con o senza l'ausilio di strumenti elettronici e comunque automatizzati secondo le modalità e le cautele previste dall'art. 13 del D.Lgs 196/2003 e conservati per il tempo necessario all'espletamento delle attività amministrative e istituzionali.

4. Strumentazione personale

4.1. Studenti

Il Regolamento di Istituto stabilisce che

L'uso dei telefonini e di altri dispositivi informatici privati con o senza auricolare, all'interno della scuola, è assolutamente vietato durante le ore di lezione. (M.P.I.): linee d'indirizzo, pag. 4, prot. N. 30 del 15.03.2007).

È concesso telefonare dal proprio apparecchio solo durante l'intervallo. In ogni altro momento il cellulare deve essere spento e conservato nello zaino, per non arrecare disturbo alle lezioni. E' vietato anche scrivere e inviare messaggi. La violazione di tale obbligo comporta le seguenti sanzioni disciplinari:

- *richiamo verbale per la prima volta;*
- *in caso di ulteriori 3 violazioni: comunicazione alla famiglia tramite sms;*
- *alla quarta violazione: nota disciplinare.*

4.4 In modo particolare, in riferimento alla direttiva n. 104 del 30.11.2007 del MPI, è fatto divieto di divulgare e inviare dati personali, senza aver prima acquisito il consenso esplicito degli interessati. È fatto quindi divieto di scattare foto o effettuare registrazioni audio e/o video all'interno dell'Istituzione Scolastica, con il proprio telefono cellulare, altrui o con altri dispositivi. L'inosservanza dell'obbligo di preventiva informazione all'interessato, comporta una sanzione amministrativa che va da un importo minimo di € 3.000 fino a € 18.000, ovvero in caso di dati sensibili o di trattamenti che comportino situazioni di pregiudizio e/o di grave detrimento anche con eventuale danno, la sanzione va da un minimo di € 5.000 fino a € 30.000.

Pertanto, nell'Istituto è consentito agli alunni di portare a scuola i telefoni cellulari, ma in caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, gli alunni potranno comunicare con le famiglie tramite gli apparecchi telefonici della scuola.

4.2. Docenti

Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili (computer di classe, iPad della scuola). 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.

4.3. Personale della scuola

Durante l'orario di servizio al restante personale scolastico l'uso del cellulare è consentito per comunicazioni personali urgenti, previa richiesta autorizzazione alla Dirigente Scolastica. L'uso di altri dispositivi elettronici personali è permesso solo per attività funzionali al servizio, e preventivamente autorizzato.

5. Prevenzione, rilevazione e gestione dei casi

5.1. Prevenzione – Rischi - Azioni

Gli insegnanti, per la natura stessa del loro lavoro, devono in molti casi fungere da “torre di avvistamento”, avamposto privilegiato delle problematiche e dei rischi che i ragazzi possono trovarsi ad affrontare ogni giorno. Responsabilità degli insegnanti è, dunque, imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tra questi, un'attenzione specifica andrà prestata ai fenomeni di:

- ▶ **bullismo/cyberbullismo** – una forma di prepotenza virtuale e non, attuata attraverso l'uso di internet e delle tecnologie digitali;
- ▶ **sexting** - pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet;
- ▶ **adescamento o grooming** – una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre i bambini/e o adolescenti a superare le resistenze

emotive e instaurare una relazione intima e/o sessualizzata; I rischi che gli alunni possono correre a scuola derivano da un uso non corretto dei dispositivi elettronici, in particolare di quelli personali.

Azioni : tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti vi sono le seguenti:

- Diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, attraverso la creazione di un'apposita area sul sito della scuola dedicata alla sicurezza in rete;
- Organizzare incontri sull'argomento.
- Richiedere 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);
- Attento monitoraggio da parte del personale docente affinché il regolamento venga rispettato;
- Tempestivo intervento tramite opportuna sanzione qualora il regolamento venga disatteso;

5.2. Rilevazione: Cosa segnalare e come segnalare

La scuola ha il dovere di monitorare le attività svolte al suo interno attraverso i dispositivi digitali, ogni docente è invitato quindi a segnalare la presenza su un dispositivo in dotazione alla scuola dei seguenti contenuti:

- Dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie o di amici, l'indirizzo di casa o il telefono, ecc.);
- Contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);

- Contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo, ecc.

Il personale della scuola, anche con l'ausilio del personale di assistenza tecnica, dovrà provvedere a conservare le eventuali tracce di una navigazione non consentita su internet o del passaggio di materiali inidonei sui pc della scuola; la data e l'ora consentiranno di condurre più approfondite

indagini; nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. Sia nel caso di chat che di messaggi di posta elettronica, l'insegnante dovrà stampare i messaggi per fornire le eventuali prove degli abusi commessi. Tali prove saranno utili anche ad informare la famiglia dell'alunno vittima di abuso, il Dirigente Scolastico e, ove si configurino reati, la Polizia Postale.

In ogni caso, sarà opportuna una tempestiva informazione delle famiglie in merito all'accaduto, anche per consentire ulteriori indagini e, in assenza di prove oggettive, di raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico ed, eventualmente, alla Polizia Postale. Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno informate tempestivamente per un confronto.

In base all'entità dei fatti si provvederà a:

- *Una comunicazione scritta tramite diario alle famiglie;*
- *Una nota disciplinare tramite registro elettronico;*
- *Una convocazione formale dei genitori degli alunni, tramite segreteria;*
- *Una convocazione delle famiglie da parte del Dirigente Scolastico.*

Per i fatti più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti. La scuola non può intervenire su ciò che gli alunni svolgono fuori da essa con strumenti digitali ma qualora il docente venisse a conoscenza di eventuali atti scorretti come la condivisione di foto non autorizzate o l'insulto da parte di un alunno ad un compagno sul gruppo classe di Whatsapp (la creazione dei gruppi classe

su WhatsApp è oggi una pratica molto diffusa) dovrà tempestivamente invitare le famiglie degli alunni coinvolti ad un attento monitoraggio delle attività svolte dai propri figli in rete.

5.3 Gestione dei casi

Per quanto riguarda la gestione dei casi il nostro Istituto ha individuato una figura referente (**prof.ssa Cenacchi per Poggio Rusco, professor Masiello per la sede di Ostiglia**). La segnalazione del caso dovrà quindi essere fatta dal singolo docente, tramite modulo allegato al presente documento (allegato 1), al/alla referente, il/la quale si occuperà di raccogliere tutte le informazioni possibili e di

segnalare l'accaduto alla Dirigente. Sarà poi la Dirigente a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti.

Definizione delle azioni da intraprendere a seconda della specificità del caso:

Casi di cyberbullismo: 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). Si tratta, pertanto, di una serie di comportamenti portati avanti ripetutamente nel tempo. Si parla di cyberbullismo quando queste forme di prevaricazione reiterate nel tempo si estendono anche alla vita online. Tale specifica forma di bullismo ha caratteristiche peculiari:

-  È pervasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
-  È un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;
-  Spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate;

Occorre tenere presente che il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamenti, se non viene aiutato ad esserne consapevole. Qualora ci si trovi di fronte ad un caso

di cyberbullismo (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà nel modo seguente:

A. Il **docente** venuto a conoscenza del fatto dovrà:

-  Informare tempestivamente la referente tramite modulo;
-  Informare tempestivamente il Consiglio di Classe dell'alunno oggetto di cyberbullismo;
-  Informare i genitori dell'alunno oggetto di cyberbullismo, offrendo loro la possibilità di avere il supporto della psicologa della scuola per affrontare al meglio la situazione;

B. I **referenti**, in collaborazione con il CdC raccoglieranno tutte le informazioni possibili;

C. Il **CdC** valuterà, a seconda della gravità del caso, come sanzionare il/i responsabili (qualora sia stato possibile individuarli); Con la collaborazione della psicologa della scuola, proporrà agli studenti attività durante le quali questi possano confrontarsi sull'accaduto;

D. La **Dirigente** valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali; Casi di sexting Con il termine sexting si intende l'invio e/o la ricezione e/o la condivisione di testi, video o immagini sessualmente esplicite tramite cellulare o tramite internet.

Qualora ci si trovi di fronte ad un caso di **sexting** (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà in maniera analoga ai casi di cyberbullismo.

Casi di adescamento online o **grooming**

Le tecnologie digitali consentono ai giovani di ampliare la propria rete di amicizie in modo quasi smisurato: non di rado gli adolescenti “concedono” la loro amicizia non solo a persone che conoscono direttamente, ma anche ad “amici di amici”. Questo li espone a rischi notevoli, come quello di dare accesso a sconosciuti al loro mondo online e quindi a informazioni personali. L'adescamento online (grooming) consiste nel tentativo, da parte di un adulto, di avvicinare un/a bambino/a o adolescente

per scopi sessuali, conquistandone la fiducia attraverso l'utilizzo della rete Internet (tramite chat, blog, forum e social networks, per esempio). In un primo tempo, l'adulto, spesso mentendo sulla propria identità e sulla propria età, mostra particolare interesse nei confronti del/la bambino/a o dell'adolescente, cercando di conquistarne la fiducia. Solo in un secondo tempo, cerca di entrare sempre più nell'intimità del bambino fino a introdurre argomenti intimi e attinenti alla sfera sessuale. È bene che anche gli insegnanti aiutino i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, per evitare che una condotta imprudente possa comportare ripercussioni non banali nella loro vita reale. Una volta riconosciuti alcuni segni che possono rinviare a una situazione di adescamento online, quali un improvviso calo nel rendimento scolastico; un aumento del tempo trascorso dall'alunno online congiunto ad una particolare riservatezza al riguardo, allusioni da parte dell'alunno alla frequentazione di una persona più grande, o a regali ricevuti, ecc., si procederà nel modo seguente.

A. Il **docente**, venuto a conoscenza del fatto, dovrà

-  Informare tempestivamente la referente tramite modulo;
-  Informare tempestivamente il Consiglio di Classe dell'alunno oggetto di adescamento;
-  Informare i genitori dell'alunno oggetto di adescamento, offrendo loro la possibilità di avere il supporto tramite Sportello d'ascolto.

B. I **referenti** in collaborazione con il CdC raccoglierà tutte le informazioni possibili;

C. Il **CdC** con la collaborazione della psicologa della scuola, proporrà agli studenti attività durante le quali gli alunni possano confrontarsi con la tematica in oggetto;

D. La **Dirigente** valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali.

6. ANNESSI

6.1 Procedure operative per la protezione dei dati personali

L'amministrazione titolare dei dati di protocollo e dei dati personali comuni, sensibili e/o giudiziari contenuti nella documentazione amministrativa di propria pertinenza dà attuazione al dettato del decreto legislativo 30 giugno 2003, n. 196, con atti formali aventi rilevanza interna ed esterna:

- ✓ Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di Protocollo Informatico e a trattare i dati di protocollo veri e propri, sono stati incaricati tramite apposito ordine di servizio;
- ✓ Relativamente agli adempimenti esterni, l'amministrazione si è organizzata per garantire che i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite; inoltre l'amministrazione certificante, in caso di accesso diretto ai propri archivi rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente;

In relazione alla protezione dei dati personali trattati al proprio interno, la Scuola dichiara di aver ottemperato a quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, con particolare riferimento:

- ☐ Al principio di necessità nel trattamento dei dati;
- ☐ Al diritto di accesso ai dati personali da parte dell'interessato;
- ☐ Alle modalità del trattamento e ai requisiti dei dati;
- ☐ All'informativa fornita agli interessati e al relativo consenso quando dovuto;
- ☐ Alla nomina degli incaricati del trattamento, per gruppo o individualmente;
- ☐ Alle misure minime di sicurezza.



<http://www.generazioniconnesse.it/site/it/home-page/>

Allegato 1

MODULO PER LA SEGNALAZIONE

(Il presente modulo va compilato dal docente che raccoglie la segnalazione con la collaborazione dello studente)

- Episodio di:
 - ☐ Bullismo
 - ☐ Cyberbullismo
 - ☐ Sexting
 - ☐ Grooming
- Alunni coinvolti:
 - Vittima/e _____
 - Responsabile/i _____
- Quando? _____
- Dove? _____

- Descrizione del fatto:

Data _____

Il docente

Allegato 2

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi

Scuola _____

Anno Scolastico _____

N°	Data	ora	Episodio (riassunto)	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		

	Status	Action	URL category
1	Enabled	Block_Denied	admin_blacklist
2	Enabled	Pass	authentication_bypass
3	Enabled	Pass	admin_whitelist
4	Enabled	Block_Denied	Unknown
5	Enabled	Pass	Advertisements & Pop-Ups
6	Enabled	Block_Denied	Alcohol & Tobacco
7	Enabled	Block_Denied	Anonymizers
8	Enabled	Pass	Arts
9	Enabled	Pass	Business
10	Enabled	Pass	Transportation
11	Enabled	Pass	Chat
12	Enabled	Pass	Forums & Newsgroups
13	Enabled	Block_Denied	Compromised
14	Enabled	Pass	Computers & Technology
15	Enabled	Block_Denied	Criminal Activity
16	Enabled	Block_Denied	Dating & Personals
17	Enabled	Block_Denied	Download Sites
18	Enabled	Pass	Education
19	Enabled	Pass	Entertainment
20	Enabled	Pass	Finance
21	Enabled	Block_Denied	Gambling
22	Enabled	Block_Denied	Games
23	Enabled	Pass	Government
24	Enabled	Block_Denied	Hate & Intolerance
25	Enabled	Pass	Health & Medicine
26	Enabled	Block_Denied	Illegal Drug
27	Enabled	Pass	Job Search
28	Enabled	Pass	Streaming Media & Downloads
29	Enabled	Pass	News
30	Enabled	Pass	Non-profits & NGOs
31	Enabled	Block_Denied	Nudity
32	Enabled	Pass	Personal Sites
33	Enabled	Block_Denied	Phishing & Fraud
34	Enabled	Pass	Politics
35	Enabled	Block_Denied	Pornography/Sexually Explicit
36	Enabled	Pass	Real Estate
37	Enabled	Pass	Religion
38	Enabled	Pass	Restaurants & Dining
39	Enabled	Pass	Search Engines & Portals
40	Enabled	Pass	Shopping
41	Enabled	Block_Denied	Social Networking
42	Enabled	Block_Denied	Spam Sites
43	Enabled	Pass	Sports
44	Enabled	Block_Denied	Malware
45	Enabled	Pass	Translators
46	Enabled	Pass	Travel
47	Enabled	Pass	Violence
48	Enabled	Block_Denied	Weapons
49	Enabled	Pass	Web-based Email
50	Enabled	Pass	General
51	Enabled	Pass	Leisure & Recreation
52	Enabled	Block_Denied	Botnets
53	Enabled	Pass	Cults
54	Enabled	Pass	Fashion & Beauty
55	Enabled	Pass	Greeting cards
56	Enabled	Block_Denied	Hacking
57	Enabled	Block_Denied	Illegal Software
58	Enabled	Pass	Image Sharing
59	Enabled	Pass	Information Security
60	Enabled	Block_Denied	Instant Messaging
61	Enabled	Block_Denied	Network Errors
62	Enabled	Block_Denied	Parked Domains
63	Enabled	Block_Denied	Peer-to-Peer
64	Enabled	Block_Denied	Private IP Addresses
65	Enabled	Block_Denied	School Cheating
66	Enabled	Pass	Sex Education
67	Enabled	Block_Denied	Tasteless
68	Enabled	Block_Denied	Child Abuse Images