



UNIONE EUROPEA

FONDI
STRUTTURALI
EUROPEI

pon
2014-2020



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)



**36° Circolo Didattico di Napoli
Scuola dell'Infanzia e Primaria statale
"Luigi Vanvitelli"**

Via Luca Giordano, 128 – 80127 – Napoli tel. 081/5567438 – Fax 081/19321086

Prot.N.1342/2020 I/04

Napoli, 31/03/2020

Ai Sigg. Genitori

A tutti i Docenti

Del 36° C.D. Napoli

-Luigi Vanvitelli-

Sito/Albo/Atti

E- Safety – Policy

Contenente

L' Informativa ai sensi degli articoli 13 e 14 del Regolamento Europeo n. 679/2016 in materia di protezione dei dati personali e successive norme nazionali di adeguamento per l'utilizzo di piattaforme necessarie per l'attuazione della DAD (Didattica A Distanza)

Aggiornata

Ai sensi della nota del Garante della Privacy del 30 Marzo 2020 avente per oggetto: **<<Coronavirus: Didattica on line, dal prime istruzioni per l'uso>>** emanata nell'intento di fornire a scuole, atenei, studenti e famiglie indicazioni utili a un utilizzo quanto più consapevole e positivo delle nuove tecnologie a fini didattici, attraverso uno specifico Atto di indirizzo che individua le implicazioni più importanti dell'attività formativa a distanza sul diritto alla protezione dei dati personali e secondo il quale *<<Le scuole e le università che utilizzano sistemi di didattica a distanza non devono richiedere il consenso al trattamento dei dati di docenti, alunni, studenti, genitori, poiché il trattamento è riconducibile alle funzioni istituzionalmente assegnate a scuole e atenei. >>*

In quanto,

<<Nella scelta e nella regolamentazione degli strumenti più utili per la realizzazione della didattica a distanza scuole e università dovranno orientarsi verso strumenti che abbiano fin dalla progettazione e per impostazioni predefinite misure a protezione dei dati.

Non è (quindi) necessaria la valutazione di impatto, prevista dal Regolamento europeo per i casi di rischi elevati, se il trattamento dei dati effettuato dalle istituzioni scolastiche e universitarie, per quanto relativo a minorenni e a lavoratori, non presenta ulteriori caratteristiche suscettibili di aggravarne i rischi. Ad esempio, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola (non, quindi, su larga scala) nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consente il monitoraggio sistematico degli utenti.>>

INDICE

1. Introduzione

- 1.1. Scopo della policy
- 1.2. Ruoli e responsabilità
- 1.3. Condivisione e comunicazione della Policy all'intera comunità scolastica
- 1.4. Gestione delle infrazioni alla policy
- 1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento
- 1.6. Integrazione della policy con regolamenti esistenti

2. Formazione e curriculum

- 2.1. Curriculum sulle competenze digitali per gli alunni
- 2.2. Formazione dei docenti sull'utilizzo e sull'integrazione delle TIC nella didattica
- 2.3. Formazione dei docenti sull'utilizzo consapevole e sicuro di internet e delle tecnologie digitali
- 2.4. Sensibilizzazione delle famiglie

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

- 3.1. Accesso ad Internet e filtri antivirus
- 3.2. Gestione accessi
- 3.3. E-mail
- 3.4. Blog e sito web della scuola
- 3.5. Classi virtuali
- 3.6. Protezione dati personali

4. Prevenzione, rilevazione e gestione dei casi

- 4.1. Rischi
- 4.2. Azioni
- 4.3. Che cosa segnalare
- 4.4. Come segnalare: quali strumenti e a chi rivolgersi
- 4.5. Definizione delle azioni da intraprendere a seconda della specificità del caso
- 4.6. Procedure operative per la gestione dei casi

5. Informativa protezione dati per utilizzo piattaforma DAD

6. Corona Virus: Didattica online, Istruzione per l'uso garante privacy

1. Introduzione

L'utilizzo delle risorse informatiche e telematiche in contesto scolastico, o comunque educativo, è divenuto ormai una priorità per il sistema educativo nazionale.

La rete è uno strumento con un indiscutibile potenziale fruibile in ambito didattico, nel campo della formazione permanente, nell'aggiornamento e per entrare in collegamento con altre realtà didattiche in Italia e nel mondo.

L'accesso alla rete a scuola costituisce un'opportunità fondamentale per migliorare la qualità della formazione ma anche per collegarla al contesto culturale e sociale. Gli studenti, infatti, grazie anche agli obiettivi del nuovo curriculum, devono imparare a trovare materiale, a recuperare documenti e scambiare informazioni utilizzando le TIC.

La scuola promuove l'utilizzo di internet per migliorare i risultati in ambito didattico, attraverso la condivisione delle risorse, l'innovazione e la comunicazione.

Dall'anno scolastico 2018/2019 il CD 36° "L. Vanvitelli" ha partecipato al progetto **"Generazioni connesse" (Safer Internet Centre Italy III)**, finanziato dalla Commissione Europea per la promozione di strategie e prassi che rendano internet un luogo più sicuro per i giovani, promuovendone un uso positivo e consapevole. Il progetto si avvale del coordinamento del Miur e della collaborazione di numerosi enti, tra i quali

- Ministero dell'Interno-Polizia Postale e delle Comunicazioni
- Autorità Garante per l'Infanzia e l'Adolescenza
- Save the Children Italia
- Telefono Azzurro
- Università degli Studi di Firenze
- Università degli studi di Roma "La Sapienza"
- Skuola.net
- Cooperativa Edi
- Movimento Difesa del Cittadino
- Agenzia Dire.

1.1. Scopo della policy

La Policy di E-Safety è un documento programmatico, redatto dal Circolo Didattico 36°, con la finalità di promuovere l'utilizzo positivo, consapevole e critico delle tecnologie all'interno della comunità scolastica. Esso contiene da un lato le norme comportamentali e le procedure di utilizzo delle TIC (Tecnologie dell'Informatica e della Comunicazione) nella didattica e nell'uso personale e ricreativo e dall'altro lato le misure di prevenzione e di gestione delle problematiche e dei rischi derivanti da un utilizzo non consapevole o scorretto delle stesse.

Gli utenti della comunità scolastica sono infatti potenzialmente esposti ai rischi della navigazione in rete: esiste infatti la possibilità di incontrare online contenuti inadeguati e /o illeciti, di subire prepotenze o abusi da contatti online (cyberbullismo, furto d'identità, grooming...) oppure ancora di scontrarsi con comportamenti illeciti e/o pericolosi (divulgazione di dati personali, web reputation, giochi online, sexting, estremismo...).

1.2. Ruoli e responsabilità

RUOLO	RESPONSABILITA'
Dirigente scolastico	<ul style="list-style-type: none"> - garantire a tutti i membri della comunità scolastica la sicurezza in rete - garantire la sicurezza del sistema informatico della scuola ed il suo monitoraggio - essere a conoscenza delle procedure da seguire in caso di infrazione della Policy - garantire un'adeguata formazione per il personale scolastico - assicurarsi che venga monitorata e implementata la E-safety policy
DSGA	<ul style="list-style-type: none"> - assicura, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione richiesti da cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate - cura la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti referenti di plesso per le TIC, provvedendo all'intervento del personale tecnico di assistenza.
Animatore digitale e team innovazione digitale	<ul style="list-style-type: none"> - promuovere e coordinare la formazione negli ambiti di sviluppo della "scuola digitale" - curare lo sviluppo del sito web della scuola - monitorare e rilevare le problematiche relative all'uso consapevole delle TIC - contribuire alla condivisione della E- Safety Policy - coinvolgere la comunità scolastica nella partecipazione ad attività e progetti attinenti la "scuola digitale" - collaborare al monitoraggio e all'implementazione della E-Safety Policy
Referente d'istituto per il bullismo e cyberbullismo	<ul style="list-style-type: none"> - monitorare e rilevare le problematiche relative all'uso sicuro di internet - contribuire alla condivisione della E- Safety Policy - promuovere e coordinare la formazione dei membri della comunità scolastica in ambito di prevenzione e contrasto del bullismo e cyberbullismo - coinvolgere la comunità scolastica nella partecipazione ad attività e progetti attinenti la prevenzione del bullismo e del cyberbullismo - diffondere la conoscenza delle procedure relative ai casi di abuso on line/cyberbullismo rilevati a scuola - collaborare al monitoraggio e all'implementazione della E-Safety Policy
I docenti	<ul style="list-style-type: none"> - informarsi, formarsi e aggiornarsi sulle problematiche attinenti la sicurezza in rete e sulla E-safety Policy adottata dalla scuola - garantire che gli alunni rispettino le regole per prevenire e contrastare l'uso scorretto e non consapevole delle Tic e della rete - guidare gli alunni affinché possano cogliere le opportunità di ricerca offerte dalla rete con consapevolezza, sviluppando le proprie competenze digitali - assicurare la riservatezza dei dati personali - vigilare sull'utilizzo da parte degli alunni (se consentito) di dispositivi mobili - segnalare all'animatore digitale qualsiasi problema o proposta di carattere tecnico organizzativo per la ricerca di soluzioni metodologiche e tecnologiche - segnalare al DS e/o al referente per il cyberbullismo qualsiasi abuso rilevato a scuola nei confronti degli alunni per l'adozione delle opportune procedure

Alunni	<ul style="list-style-type: none"> - essere consapevoli e responsabili nell'utilizzo delle TIC e della rete, in relazione alla propria età e alle proprie conoscenze, comprendendo l'importanza della sicurezza - adottare condotte rispettose degli altri anche nella comunicazione in rete - esprimere dubbi e /o difficoltà o richieste d'aiuto riguardo alla rete o alle TIC a docenti e /o genitori - conoscere la E-Safety Policy della scuola
Genitori	<ul style="list-style-type: none"> - conoscere, condividere e sostenere la E - Safety Policy della scuola - seguire i propri figli anche a casa nel loro utilizzo delle TIC, dei dispositivi e della rete sia nell'uso didattico che ricreativo, condividendo con essi regole di utilizzo - condividere con i docenti le linee educative d'intervento in relazione ad eventuali problemi
Personale scolastico	<ul style="list-style-type: none"> - conoscere, comprendere e condividere la E-Safety Policy della scuola - segnalare qualsiasi abuso sospetto o problema ai responsabili - assumere comportamenti sicuri e responsabili nell'uso delle Tic e della rete

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

La E - Safety Policy è rivolta a tutti i membri della comunità scolastica e pertanto dovrà essere conosciuta e condivisa da tutti. La Policy sarà comunicata e condivisa con le seguenti modalità:

- discussione all'interno degli organi collegiali e pubblicazione del documento sul sito della scuola
- presentazione del documento ai genitori e agli alunni, all'inizio del primo anno di ogni ciclo scolastico
- sensibilizzazione attraverso attività, laboratori, incontri formativi, spettacoli che portino a riflettere su rischi e opportunità del web
- segnalazione e pubblicazione sul sito di materiale informativo specifico e aggiornato

1.4. Gestione delle infrazioni alla policy

Per gli alunni: le possibili infrazioni in cui è possibile che gli studenti incorrano a scuola nell'uso delle Tic e della rete possono essere verosimilmente le seguenti:

- utilizzo della rete per una comunicazione scorretta nei confronti di altri
- utilizzo irresponsabile e incauto di foto o dati personali
- condivisione di immagini intime o dal contenuto esplicito
- comunicazione con sconosciuti
- collegamento a siti non indicati dai docenti e /o inadeguati

Gli interventi previsti devono essere rapportati all'età e allo sviluppo cognitivo ed avere sempre intento educativo, di rinforzo di comportamenti corretti e riparativi di eventuali danni causati, fatti salvi naturalmente i casi di reato che devono essere adeguatamente segnalati alle autorità competenti. Eventuali denunce per cyberbullismo saranno trattate secondo la normativa vigente.

Ogni intervento deve essere un'occasione di ri-definizione delle regole sociali, di promozione di una corretta gestione dei conflitti e delle proprie emozioni.

- richiamo verbale
- richiamo scritto sul registro/libretto delle comunicazioni, con sospensione dell'attività svolta (ad esempio attività di ricerca al pc) o ritiro del cellulare fino a fine giornata verbale
- convocazione dei genitori da parte dei docenti
- convocazione dei genitori da parte del DS

Per il personale scolastico: Il personale scolastico potrebbe presumibilmente incorrere nelle seguenti infrazioni:

- utilizzo della rete e delle TIC non riguardante l'attività didattica e/o professionale, anche tramite salvataggio di materiale o installazione di software non idonei
- trattamento dei dati non conforme ai principi riguardanti la privacy
- diffusione delle password di protezione e custodia non adeguata degli strumenti informatici
- mancata vigilanza nell'uso delle TIC da parte degli alunni
- mancata segnalazione di situazioni critiche al DS

Il DS può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza. Tutto il personale è tenuto a collaborare con il DS in caso di avvio di procedure che possono avere rilevanza diversa (organizzativa, disciplinare, amministrativa, penale) a seconda della gravità delle infrazioni segnalate. Le procedure sono quelle previste per legge e dal contratto di lavoro.

Per i genitori: Alla luce dell'abbassamento dell'età media alla quale i ragazzi si accostano all'utilizzo dello smartphone, del pc o di altri dispositivi, si ritiene fondamentale il ruolo educativo della famiglia nell'impartire agli studenti alcune fondamentali regole, che favoriscano l'uso consapevole e corretto delle TIC, sia a casa che a scuola, per un uso didattico e/o personale. Si suggeriscono pertanto alcune semplici regole:

- posizionare il computer in una stanza della propria casa in cui sia ben visibile a tutti quando viene utilizzato,
- non concedere al proprio figlio troppa autonomia nell'utilizzo dello smartphone e/o del computer,
- non condividere l'utilizzo dei propri dispositivi con i ragazzi se si conservano in memoria materiali non idonei,
- dotare i dispositivi dei ragazzi di sistemi di sicurezza e/o controllo.

In caso di infrazioni alla policy da parte degli studenti inoltre i genitori possono essere convocati a scuola per condividere strategie educative nuove e più efficaci.

Naturalmente i genitori risponderanno della condotta dei propri figli nei casi previsti dalla legge vigente.

1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il monitoraggio della E-safety policy avverrà ogni anno scolastico: sarà cura del DS, con la collaborazione dell'Animatore Digitale, del docente referente per il cyberbullismo e degli organi collegiali, rilevare periodicamente l'impatto della Policy, i cambiamenti significativi e le eventuali necessità di miglioramento e/o aggiornamento.

1.6. Integrazione della policy con regolamenti esistenti

La Policy si integra al Regolamento d'Istituto quanto a norme comportamentali relative all'utilizzo delle dotazioni informatiche della scuola, dei laboratori, della rete e del traffico dati.

2. Formazione e curriculum

2.1. Curriculum sulle competenze digitali per gli alunni

La “RACCOMANDAZIONE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 18 dicembre 2006 relativa a competenze chiave per l'apprendimento permanente (2006/962/CE)” riporta la seguente definizione di Competenza digitale: “La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet.”

Tale documento sottolinea inoltre che “La competenza digitale presuppone una solida consapevolezza e conoscenza della natura, del ruolo e delle opportunità delle TSI nel quotidiano: nella vita privata e sociale come anche al lavoro. In ciò rientrano le principali applicazioni informatiche come trattamento di testi, fogli elettronici, banche dati, memorizzazione e gestione delle informazioni oltre a una consapevolezza delle opportunità e dei potenziali rischi di Internet e della comunicazione tramite i supporti elettronici (e-mail, strumenti della rete) per il lavoro, il tempo libero, la condivisione di informazioni e le reti collaborative, l'apprendimento e la ricerca. Le persone dovrebbero anche essere consapevoli di come le TSI possono coadiuvare la creatività e l'innovazione e rendersi conto delle problematiche legate alla validità e all'affidabilità delle informazioni disponibili e dei principi giuridici ed etici che si pongono nell'uso interattivo delle TSI. Le abilità necessarie comprendono: la capacità di cercare, raccogliere e trattare le informazioni e di usarle in modo critico e sistematico.

Tale documento sottolinea inoltre che “La competenza digitale presuppone una solida consapevolezza e conoscenza della natura, del ruolo e delle opportunità delle TSI nel quotidiano: nella vita privata e sociale come anche al lavoro. In ciò rientrano le principali applicazioni informatiche come trattamento di testi, fogli elettronici, banche dati, memorizzazione e gestione delle informazioni oltre a una consapevolezza delle opportunità e dei potenziali rischi di Internet e della comunicazione tramite i supporti elettronici (e-mail, strumenti della rete) per il lavoro, il tempo libero, la condivisione di informazioni e le reti collaborative, l'apprendimento e la ricerca. Le persone dovrebbero anche essere consapevoli di come le TSI possono coadiuvare la creatività e l'innovazione e rendersi conto delle problematiche legate alla validità e all'affidabilità delle informazioni disponibili e dei principi giuridici ed etici che si pongono nell'uso interattivo delle TSI. Le abilità necessarie comprendono: la capacità di cercare, raccogliere e trattare le informazioni e di usarle in modo critico e sistematico, accertandone la pertinenza e distinguendo il reale dal virtuale pur riconoscendone le correlazioni. Le persone dovrebbero anche essere capaci di usare strumenti per produrre, presentare e comprendere informazioni complesse ed essere in grado di accedere ai servizi basati su Internet, farvi ricerche e usarli.

Le persone dovrebbero anche essere capaci di usare le TSI a sostegno del pensiero critico, della creatività e dell'innovazione. L'uso delle TSI comporta un'attitudine critica e riflessiva nei confronti delle informazioni disponibili e un uso responsabile dei mezzi di comunicazione interattivi. Anche un interesse a impegnarsi in comunità e reti a fini culturali, sociali e/o professionali serve a rafforzare tale competenza.” L'acquisizione della competenza digitale è trasversale alle discipline ed è promossa da tutti i docenti durante le attività di insegnamento quotidiane. Le competenze digitali vengono certificate in uscita, sia al termine della Scuola Primaria che Secondaria di primo grado. Nell'ambito della prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo gli studenti hanno partecipato a incontri con esperti esterni, destinati a classi selezionate nell'ambito del progetto d'Istituto.

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

In conformità con i commi 57 e 58 della legge 107 il Circolo Didattico 36° aderisce al Piano Nazionale per la Scuola digitale.

Il Team per l'innovazione digitale, costituito dunque da 6 docenti, ha la funzione di supportare e accompagnare l'innovazione didattica nell'istituzione scolastica e l'attività dell'Animatore digitale, che avvierà delle attività nei seguenti ambiti, secondo quanto indicato dal Miur:

1. **FORMAZIONE INTERNA:** stimolare la formazione interna alla scuola sui temi del PNSD, attraverso l'organizzazione e la coordinazione di laboratori formativi (senza essere necessariamente un formatore), favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative.
2. **COINVOLGIMENTO DELLA COMUNITÀ SCOLASTICA:** favorire la partecipazione e stimolare il protagonismo degli alunni nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, anche aprendo i momenti formativi alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa.
3. **CREAZIONE DI SOLUZIONI INNOVATIVE:** individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; la pratica di una metodologia comune; informazione su innovazioni esistenti in altre scuole), coerenti con l'analisi dei fabbisogni della scuola stessa.

Per quanto riguarda la formazione esterna inoltre, la scuola promuove la partecipazione a convegni, seminari, workshop e corsi d'aggiornamento oltre ad aderire a progetti di formazione curati da associazioni o enti.

2.3. Formazione dei docenti sull'utilizzo consapevole e sicuro di internet e delle tecnologie digitali

La formazione dei docenti sull'utilizzo consapevole e sicuro di Internet può essere affidata all'autoaggiornamento, a momenti di formazione individuale o collettiva. In particolare durante il triennio 2019/22 i docenti parteciperanno alle attività di Formazione sulla materia, ritenute di importanza strategica per stare al passo con lo sviluppo delle avanguardie educative.

La partecipazione del Circolo Didattico 36° al progetto "Generazioni Connesse" prevede una fase di autoaggiornamento dei docenti accedendo all'area docenti del sito di Generazioni Connesse e consultando il materiale informativo e didattico in esso contenuto.

2.4. Sensibilizzazione delle famiglie

La condivisione di questo documento e del Patto di corresponsabilità sarà occasione di confronto con le famiglie e di sensibilizzazione dei genitori all'importanza di un uso consapevole delle TIC e della rete, al fine di prevenire i possibili rischi. Sul sito della scuola saranno pubblicati materiali informativi dedicati ai genitori.

Nell'ambito della prevenzione e contrasto del cyberbullismo gli alunni della scuola Primaria, nell'a.s.2017/2018 hanno potuto partecipare ad un incontro formativo dal titolo "T.E.T.I.", promosso dalla scuola in collaborazione con la Polizia di Stato.

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

3.1. Accesso ad Internet e filtri antivirus

L'accesso ad internet è possibile nelle aule dotate di Lim o video proiettore nei laboratori multimediali.

L'accesso è schermato da filtri opportuni che impediscono il collegamento a siti appartenenti a black list, secondo le impostazioni fornite dall'Amministratore Digitale, che provvede periodicamente all'aggiornamento del sistema informatico, avvalendosi di tecnici esterni.

3.2. Gestione accessi (password, backup, ecc)

L'accesso ad internet per i docenti nelle aule è vincolato ad una password.

Nel laboratorio multimediale è possibile accedere ad internet anche mediante cavo LAN.

Non vi è un back up dei file elaborati se non quello effettuato dagli utenti sui propri dispositivi USB rimovibili o in apposite cartelle di documenti.

3.3. E-mail e uso delle Google Apps for Education

Tutto il personale docente del Circolo Didattico 36° è dotato di un accesso riservato personale al sito della scuola, compatibile con le norme sulla privacy, per assicurare modalità di comunicazione corrette ed efficaci all'interno dello stesso.

Si invita pertanto il personale docente a consultare quotidianamente la propria area riservata.

3.4. Blog e sito web della scuola

La scuola ha attualmente un sito web: www.scuolavanvitelli36.gov.it

Il Dirigente Scolastico valuta la sicurezza e l'adeguatezza dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy. Il Circolo Didattico 36° non ha un proprio Blog.

3.5. Classi virtuali

La scuola non ha posto alcun vincolo alla creazione di classi virtuali in cui vengano registrati gli alunni per realizzare attività didattiche di flipped classroom o formazione a distanza o condivisioni di documenti per lavori di gruppo. Trattandosi però di soggetti minori di 14 anni si richiede l'autorizzazione dei genitori ad essere iscritti in una classe virtuale qualora la piattaforma scelta preveda l'uso di un indirizzo email per la registrazione.

3.6. Protezione dati personali

Il personale scolastico è "incaricato del trattamento" dei dati personali degli utenti (alunni, genitori, ecc), nei limiti delle operazioni necessarie ai fini dello svolgimento della propria funzione. Tutto il personale incaricato riceve istruzioni applicabili al trattamento dei dati personali su supporto cartaceo e/o informatico, ai fini della protezione degli stessi. Viene inoltre fornita ai genitori lettera informativa e viene richiesta l'autorizzazione all'utilizzo dei dati personali degli alunni, fatti salvi i trattamenti istituzionali obbligatori.

Viene, inoltre, richiesta ai genitori/tutori, all'inizio di ogni anno scolastico, una dichiarazione liberatoria per la pubblicazione di elaborati, nomi, voci, immagini e materiali audiovisivi degli alunni.

4. Prevenzione, rilevazione e gestione dei casi

4.1. Rischi

I rischi che gli alunni possono correre a scuola nell'utilizzo delle TIC risiedono principalmente nell'uso scorretto o inconsapevole del proprio smartphone, dei propri dispositivi o dei pc collegati in rete della scuola.

Lo smartphone non è richiesto per le attività didattiche ed il suo utilizzo è disciplinato da circolari interne alla scuola. In alcuni casi agli studenti è permesso l'utilizzo dei propri device per scopi didattici (per es. alunni BES, alunni diversamente abili).

Gli studenti, eludendo la sorveglianza dei docenti, potrebbero con i propri smartphone, con i propri dispositivi o con i pc della scuola parlare o scrivere ai genitori, scaricare o spedire o postare foto personali o addirittura intime, proprie o altrui, scaricare, inviare o postare video con contenuti non adatti (violenti o indecenti), accedere a videogiochi o a siti vietati o non consigliati ai minori, ascoltare musica dai contenuti espliciti, inviare o ricevere messaggi molesti o minacciosi, chattare con sconosciuti..

4.2. Azioni

Le azioni che la scuola può prevedere per la prevenzione dei rischi sono le seguenti:

- Disciplinare l'uso dello smartphone a scuola, vietandone l'uso ad eccezione di casi particolari, quali visite guidate, e comunque sotto la supervisione del docente responsabile;
- Sensibilizzare e formare tutti gli attori della vita scolastica (alunni, genitori, docenti, personale scolastico) riguardo ai potenziali rischi connessi all'uso delle TIC,
- Richiedere ai genitori l'autorizzazione al trattamento dei dati personali eccedenti quelli istituzionali obbligatori;
- Utilizzare software che impediscono il collegamento ai siti web per adulti;
- Nei laboratori centralizzare il blocco dei siti web sul server del docente, in modo che possa intercettare ed eventualmente respingere le richieste di connessione da parte dei client.
- Integrare il regolamento dell'Istituto ed il Patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti.

Le azioni previste nella recente legge 29 maggio 2017, n.71 per il contenimento degli incidenti sono le seguenti:

- “Ciascun genitore o soggetto esercente la responsabilità del minore che abbia subito taluno degli atti di cui all'art.1, comma 2, della presente legge, (atti quindi di cyberbullismo) può inoltrare al titolare del trattamento o al gestore del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato del minore...”
- “Qualora, entro le ventiquattro ore successive al ricevimento dell'istanza di cui al comma 1, il soggetto responsabile non abbia comunicato di avere assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco richiesto, ed entro quarantotto ore non vi abbia provveduto, o comunque nel caso in cui non sia possibile identificare il titolare del trattamento o il gestore del sito internet o del social media, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali, il quale, entro quarantotto ore dal ricevimento della richiesta, provvede ai sensi degli articoli 143 e 144 del citato decreto legislativo 30 giugno 2003, n. 196. “
- “Salvo che il fatto costituisca reato, in applicazione della normativa vigente e delle disposizioni di cui al comma 2, il dirigente scolastico che venga a conoscenza di atti di cyberbullismo ne informa tempestivamente i soggetti esercenti la responsabilità genitoriale ovvero i tutori dei minori coinvolti e attiva adeguate azioni di carattere educativo.”
- I casi di reato devono essere tempestivamente denunciati alle autorità competenti.

4.3. Che cosa segnalare

Gli alunni potrebbero riferire spontaneamente al docente, al genitore o a qualche compagno che si fa portavoce, stati di an-sia, tristezza, risentimento o paura derivanti da situazioni di rischio connesse all'uso delle TIC. I fatti riferiti potrebbero essere accaduti a scuola o al di fuori della scuola. Le prove di quanto riferito potrebbero essere presenti nella memoria dei dispositivi utilizzati e potrebbero essere mostrati spontaneamente dall'alunno, dal genitore o notati dal docente che si accorgesse di una infrazione in corso. Il docente può sempre controllare la strumentazione della scuola, mentre per controllare i dispositivi dell'alunno deve rivolgersi al genitore.

I contenuti che devono essere ritenuti “pericolosi”, e quindi segnalati per tutelare l’interesse superiore del minore, in quanto comunicati, pubblicati, ricevuti, scaricati in rete, possono essere i seguenti:

- Contenuti personali (dati personali quali immagini, recapiti telefonici, informazioni private, indirizzo, ecc)
- Contenuti violenti o aggressivi (minacce, informazioni false, immagini o video con contenuto inneggiante alla violenza, al suicidio, al razzismo, immagini o video umilianti, insultanti, imbarazzanti, ecc)
- Contenuti a sfondo sessuale (messaggi molesti, conversazioni che dimostrino una relazione intima, foto o video con nudità o abbigliamento succinto, immagini o video pornografici o pedo pornografici, ecc)

4.4. Come segnalare: quali strumenti e a chi rivolgersi

Per quanto riguarda il telefono cellulare o i dispositivi personali ci si può assicurare che l’alunno vittima di comportamenti scorretti salvi ogni conversazione e /o immagine, in modo da poter visualizzare il numero del mittente.

Per quanto riguarda invece i pc della scuola si può provvedere a conservare le prove della condotta scorretta o dell’abuso salvando e/o stampando con data e ora il contenuto dei messaggi, e, se possibile, l’ID del mittente, l’indirizzo del sito web, eccetera. Conservare la prova è utile, se non indispensabile, per rendere noto l’accaduto al Dirigente Scolastico, ai genitori degli alunni e, nei casi di reato, alle autorità competenti.

Qualora non si disponga di prove, ma solo delle testimonianze dell’alunno, magari relativamente a fatti accaduti fuori dal contesto scolastico, è comunque opportuno comunicare le notizie raccolte al DS, ai genitori dell’alunno o degli alunni coinvolti (vittima e autore della condotta scorretta) ed in caso di sospetto reato alle autorità competenti.

Per le segnalazioni sono previsti i seguenti strumenti:

- Relazione scritta al Ds
- Annotazione scritta del comportamento sul registro e comunicazione scritta ai genitori sul libretto, con restituzione controfirmata
- Convocazione scritta e colloquio con i genitori

Le comunicazioni formali possono essere anticipate per maggiore celerità da comunicazioni informali.

4.5. Definizione delle azioni da intraprendere a seconda della specificità del caso

Gestione dei casi di “immaturità”

Può sembrare naturale all’alunno fornire i propri dati sui siti allestiti in modo tale da attrarre l’attenzione dei bambini, con giochi e animazioni, personaggi simpatici e divertenti, che richiedono una procedura di registrazione. Curiosità, manifestazioni di reciproco interesse tra pari, idee e fantasie sulla sessualità sono espressione da una parte del progressivo sviluppo socio-affettivo dell’alunno e dall’altra dei molteplici messaggi espliciti che gli giungono quotidiana-mente attraverso i media (televisione, DVD, internet, giornali e riviste), i discorsi degli altri bambini o degli adulti. I comportamenti cosiddetti “quasi aggressivi”, che spesso si verificano tra coetanei, le interazioni animate o i contrasti verbali, o la presa in giro “per gioco”, effettuata anche in rete, mettono alla prova la relazione con i compagni, la supremazia o la parità tra i soggetti implicati e l’alternanza e sperimentazione dei diversi ruoli. Il gruppo dei pari rappresenta anche il momento di conquista dell’autonomia dall’adulto e pertanto luogo di “complicità” e di piccole “trasgressioni”, di scambi “confidenziali” condivisi fra gli amici nella rete o con il cellulare. Detti comportamenti, che finiscono per

arrivare all'attenzione degli adulti, sono controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza civile e democratica, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.

Gestione dei casi di “prepotenza” o “prevaricazione”

I comportamenti definibili “Bullismo” possono esprimersi nelle forme più varie e non sono tratteggiabili a priori; se non contestualizzandoli. Le caratteristiche che aiutano a individuarli e a distinguerli dallo scherzo, dalle intemperanze caratteriali, dai diverbi usuali fra i ragazzi sono la costanza nel tempo e la ripetitività, l'asimmetria (disuguaglianza di forza e di potere), il disagio della/e vittima/e. Il bullismo si esplica infatti con comportamenti e atteggiamenti costanti e ripetitivi di arroganza, prepotenza, prevaricazione, disprezzo, dileggio, emarginazione, esclusione ai danni di una o più persone, agiti da un solo soggetto, ma in genere da un gruppo.

Nel caso particolare del Cyberbullismo le molestie sono attuate attraverso strumenti tecnologici:

- invio di sms, messaggi in chat, e-mail offensive o di minaccia;
- diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o email nelle mailing-list o nelle chat-lin
- pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata.

Il bullismo in particolare può originarsi anche dall'exasperazione di conflitti presenti nel contesto scolastico. Il conflitto, presente in ogni normale intenzione, è da considerarsi come un campanello d'allarme e può degenerare in forme patologiche quando non lo si riconosce e gestisce in un'ottica evolutiva dei rapporti, di negoziazione e risoluzione. Se non gestito positivamente, infatti, il conflitto rischia di mutarsi e provocare effetti distruttivi sulle relazioni (prevaricazione e sofferenza) e sull'ambiente (alterazione del clima del gruppo-classe). In considerazione dell'età degli alunni considerati possono prefigurarsi alcune forme di interazioni che possono evolvere verso tale fenomeno. Per prevenire e affrontare il bullismo dunque i docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, coinvolgendo i genitori degli allievi. L'elemento fondamentale per una buona riuscita dell'intervento educativo è infatti la corretta, compiuta e convinta ristrutturazione dell'ambiente sociale in cui tale fenomeno si verifica, e in particolare delle relazioni nel contesto della classe. Gli atteggiamenti degli alunni, così come quelli dei loro genitori, possono giocare un molto significativo nel ridurre la dimensione del fenomeno. Gli interventi mirati sul gruppo classe sono gestiti in collaborazione dal team dei docenti della classe e d'intesa con le famiglie - ad esempio con percorsi di mediazione volta alla gestione positiva del conflitto, con gruppi di discussione (circle time), con rappresentazioni e attività di role-play sull'argomento del bullismo, con le strategie del problem solving. Vengono intrapresi anche i percorsi individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali. Anche in relazione alle manifestazioni socio-affettive fra pari, al linguaggio sessualizzato o “volgare”, al fine di evitare prevaricazioni e imbarazzo o disagio, i docenti intervengono per favorire nei bambini un buon rapporto con il proprio corpo e per far percepire meglio eventuali violazioni dei limiti di prossimità o di “confidenza” ed imparare ad opporvisi, per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito e determinazione nel rifiutare i contatti anche “a distanza” sgradevoli o “strani”, per rendere consapevoli gli alunni del diritto al rispetto dei propri limiti e di quelli altrui, per far capire ai ragazzi che l'interazione on-line deve sottostare a delle regole di buon comportamento, né più né meno della comunicazione a viso aperto, quale quella della vita reale. Inoltre la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia altresì di servirsi dello sportello di ascolto psicologico gratuito se attivo presso la scuola. Promuove e supporta la richiesta delle famiglie

rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi comunali e alla ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).

Gestione degli “abusi sessuali”

“In generale si parla di abuso sessuale sui bambini quando un bambino viene coinvolto in un atto sessuale. Ciò è caratterizzato dal fatto che il bambino non comprende del tutto tale atto, non è informato e quindi non è in grado di acconsentire, oppure sulla base del suo livello di sviluppo non è ancora pronto per tale atto e non può dare il proprio consenso”. Lo spettro delle forme di abuso e di violenza è diventato ancora più ampio e subdolo in seguito alle possibilità offerte dai nuovi mezzi di comunicazione come internet, il cellulare o altri dispositivi tecnologici, e il loro utilizzo sempre più diffuso non fa che acuire il problema. Internet, infatti, permette di scaricare o vendere immagini o filmati di pornografia infantile. Succede sempre più frequentemente che un adulto prenda contatto con dei bambini nei forum o nelle chat su internet, e che li metta di fronte a domande o messaggi sessuali o addirittura a immagini pornografiche. A volte l'adulto induce i bambini a spogliarsi davanti alla webcam oppure a inviare una fotografia che li ritrae nudi tramite internet o sul cellulare, per poi ricattarli e costringerli a non rivelare gli abusi. Spesso l'adulto finge di essere minorenne. La denuncia all'autorità giudiziaria o agli organi di Polizia, da parte degli insegnanti o del Dirigente Scolastico, costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole. La presa in carico di situazioni di abuso sessuale, così delicate e complesse, richiede un approccio multidisciplinare, da parte di diverse figure professionali. I versanti su cui si articola l'intervento possono essere essenzialmente tre: medico, socio-psicologico e giudiziario. Il compito della scuola non è comunque solo quello di “segnalare”, ma più ampio ed importante, soprattutto nella prevenzione dell'abuso, nonché nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali ed educativi che possono aiutare il bambino a riprendere una crescita serena. A tal fine la scuola lavora insieme alle altre figure professionali e alle famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo le occasioni di confronto e di dialogo.

In particolare nel caso in cui ci si dovesse imbattere in materiale pedopornografico (cioè contenuti foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali), è necessario, innanzitutto, evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto. Ciò è reato per chiunque. Nel venire a conoscenza di materiali di questo tipo è importante contribuire alla loro eliminazione: basta inserire le informazioni richieste sugli appositi moduli online, disponibili ai siti

www.stop-it.it

<http://www.azzurro.it/it/clicca-esegнала>”

ovvero collegandosi al sito della polizia postale

<https://www.commissariatodips.it>,

ove è possibile sia segnalare che denunciare. In alternativa è possibile recarsi nella sede più vicina della polizia giudiziaria.

Ciò consente di operare con la massima tempestività. Non operare in modo isolato, ma confrontarsi con i colleghi di classe e il Dirigente Scolastico.

4.6. Procedure operative per la gestione dei casi

LINEE GUIDA PER ALUNNI

- Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere caratteri speciali;
- Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola;
- Non inviare a nessuno fotografie tue o di tuoi amici;
- Prima di inviare o pubblicare su un BLOG la fotografia di qualcuno, chiedi sempre il permesso;
- Chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da Internet;
- Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola;
- Quando sei connesso alla rete RISPETTA SEMPRE GLI ALTRI, ciò che per te è un gioco o uno scherzo può rivelarsi offensivo per qualcun altro;
- Non rispondere alle offese ed agli insulti;
- Blocca i Bulli: molti Blog e siti social network ti permettono di segnalare i cyberbulli;
- Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto;
- Se ricevi materiale offensivo (e-mail, sms, mms, video, foto, messaggi vocali) non diffonderlo: potresti essere accusato di cyberbullismo;
- Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE;
- Riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet;
- Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori;
- Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che di-cono di essere;
- Non è consigliabile inviare mail personali, perciò rivolgiti sempre al tuo insegnante prima di inviare messaggi di classe o ai tuoi genitori prima di inviare messaggi da casa;
- Non scaricare (download) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori;
- Non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso del tuo insegnante o dei tuoi genitori.

LINEE GUIDA PER INSEGNANTI

- Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune;
- Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi per la macchina e al di fuori delle cartelle personali;
- Discutete con gli alunni della policy e-safety della scuola, di utilizzo consentito della rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet;
- Date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informa-teli che le navigazioni saranno monitorate;
- Ricordate di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione su Internet del laboratorio (qualora sia stata attivata);
- Ricordate agli alunni che la violazione consapevole della policy e-safety della scuola, di utilizzo consentito della rete, comporta sanzioni di diverso tipo;
- Adottate provvedimenti "disciplinari", proporzionati all'età e alla gravità del comportamento;
- Adottati interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ridefinizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni;
- Nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi (sportello di ascolto psicologico gratuito se attivo presso la scuola, Servizi Sociali per la fruizione di servizi socio-educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare);
- Chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indirizzo e-mail, ecc....;
- Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro;
- In caso di abuso sessuale rilevato anche attraverso i nuovi mezzi di comunicazione come internet o il cellulare, confrontatevi con i colleghi di classe e il Dirigente Scolastico, denunciate all'autorità giudiziaria o a-gli organi di Polizia.

CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA

CONSIGLI GENERALI

Posizionate il computer in salone o in una stanza accessibile a tutta la famiglia;

Evitate di lasciare le e-mail o file personali sui computer di uso comune;

Concordate con vostro figlio le regole: quando si può usare internet e per quanto tempo...

Inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l'accesso a siti porno-grafici;

Aumentate il filtro del "parental control" attraverso la sezione sicurezza in internet dal pannello di control-lo;

Attivate il firewall (protezione contro malware) e antivirus;

Mostratevi coinvolti: chiedete a vostro figlio di mostrarvi come funziona internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante;

Incoraggiate le attività on-line di alta qualità: ricercare informazioni scientifiche, ricercare nuovi amici nel mondo;

Partecipate alle esperienze on-line: navigate insieme a vostro figlio, incontrate gli amici online, discutete degli eventuali problemi che si presentano;

Comunicare elettronicamente con vostro figlio: inviate, frequentemente, E-mail, Instant Message (IM);

Spiegate a vostro figlio che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai fornita ai compagni o ad altre persone;

Stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia);

Discutete sul tema dello scaricare file e della possibilità di ricevere file con virus;

Raccomandate di non scaricare file da siti sconosciuti;

Incoraggiate vostro figlio a dirvi se vedono immagini particolari o se ricevono e-mail indesiderate;

Discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie;

Spiegate a vostro figlio che le password, i codici pin, i numeri di carta di credito e i numeri di telefono e i dettagli degli indirizzi e-mail sono privati e non devono essere dati ad alcuno;

Spiegate a vostro figlio che non tutti in Internet sono chi realmente dichiarano di essere; di conseguenza i vostri ragazzi non dovrebbero mai accordarsi per appuntamenti senza consultarvi prima;

Il modo migliore per proteggere vostro figlio è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

Consigli in base all'età

Se tuo figlio ha meno di 8 anni

Seleziona con molta attenzione i siti “sicuri”: ricordati che i gestori dei siti, per trarre il massimo guadagno, permettono agli inserzionisti di pubblicizzare i propri prodotti;

Comunica a tuo figlio tre semplici regole:

non dare il tuo vero nome, indirizzo e numero di telefono. Usa sempre il tuo “computer username” o nickname;

se compare sullo schermo qualche messaggio o banner, chiudilo: insegna a tuo figlio come si fa;

naviga esclusivamente sui siti autorizzati dai genitori: se vuoi andare su un nuovo sito, dobbiamo andarci INSIEME (molti siti richiedono la registrazione. Insegna a tuo figlio come registrarsi senza rivelare informazioni personali).

Se tuo figlio ha tra gli 8 anni e i 10 anni

Progressivamente diminuisci la supervisione: dagli otto ai dieci anni permetti a tuo figlio di navigare da solo nei siti autorizzati, sottolineando che deve consultarti prima di esplorarne dei nuovi.

Verifica periodicamente i contenuti dei siti “sicuri”.

Discuti con tuo figlio i rischi che possono presentarsi durante la navigazione on-line.

Controlla, dalla cronologia il menu navigazione, se tuo figlio ha consultato siti non autorizzati per i quali non ti ha chiesto il permesso.

Supervisiona l’email di tuo figlio dopo averlo reso consapevole del fatto che hai pieno accesso alle sue comunicazioni.

Se tuo figlio vuole usare IM verifica che i suoi contatti siano limitati agli amici conosciuti.

Specifica che non può inserire nuovi contatti senza averti prima consultato.

Comunicagli che è assolutamente vietato cliccare su un link, contenuto in una E-mail, su un pop-up pubblicitario o su un banner (ricordati, infatti, che potrebbero presentarsi immagini pornografiche o che potrebbe avviarsi il download di “malware”) . Incoraggia l’uso di internet per svolgere ricerche scolastiche.

Definisci il tempo massimo di connessione ed incoraggia le attività con il mondo reale.

Se tuo figlio ha tra gli 11 anni e i 13 anni

Tuo figlio è diventato grande e potrebbe dirti che il suo migliore amico ha la possibilità di navigare tutti i giorni a tutte le ore Che fare?

Crea una partnership con i genitori dei migliori amici di tuo figlio in modo da concordare con loro le regole: tempi di connessione, fasce orarie, siti autorizzati, modalità di utilizzo di IM (messaggistica istantanea).

Aiuta tuo figlio a creare una rete on-line sicura: siti controllati ed amici conosciuti.

Se tuo figlio ha oltre 13 anni

Verifica i profili di tuo figlio e dei suoi amici, nei siti cerca persona, informandolo dei tuoi periodici controlli.

Ricordati che in questa fascia di età aumentano le ricerche di materiale sessuale ed i rischi di seduzioni sessuali on-line da parte di cyberpredatori adulti: condividi con tuo figlio le procedure per navigare in sicurezza ed evitare on-line ed off-line brutti incontri.

Confrontati con tuo figlio su tutti questi rischi e se protesta per il controllo, ribadisci che è un dovere del genitore supervisionare e monitorare l'uso di internet.

Stringi un accordo: se tuo figlio dimostra di avere compreso i rischi e di sapere e volere usare internet in modo si-curo, diminuisci la supervisione.

Il computer deve rimanere in salone o in una stanza accessibile a tutta la famiglia e non nella camera di tuo figlio ALMENO fino ai 16 anni.



**36° CIRCOLO DIDATTICO SCUOLA DELL'INFANZIA E PRIMARIA
"LUIGI VANVITELLI"**

Via Luca Giordano,128 - 80128 - NAPOLI Tel. 081/5567438 Fax 081/ 19321086
@-mail:nae03600t@istruzione.it web site : www.scuolavanvitelli36.gov.it

Informativa ai sensi degli articoli 13 e 14 del Regolamento Europeo n. 679/2016 in materia di protezione dei dati personali e successive norme nazionali di adeguamento per l'utilizzo di piattaforme DAD (Didattica A Distanza)

Con il DPCM del 8 marzo 2020, che comunicava la sospensione delle attività didattiche di ogni ordine e grado, e con la comunicazione n. 279 del 09/03/2020 del MIUR, con la quale si dettavano le indicazioni per l'attuazione della didattica a distanza, il 36° Circolo Didattico L. Vanvitelli, ha acquisito per tramite dei docenti, delle rappresentanti di classe e dei membri del Consiglio di Circolo, le liberatorie per l'attivazione, per tutte le classi, dei servizi della piattaforma EDMODO.

L'adesione a tale piattaforma ha consentito agli studenti ed ai docenti del Circolo di usufruire gratuitamente di una serie di servizi per la didattica a distanza quali: classi virtuali, cloud, forum, servizi di messaggistica, etc.

L'obiettivo di questa iniziativa è ottimizzare, attraverso le tecnologie di rete, l'attività didattica e la circolazione delle informazioni interne, come comunicazioni, documentazione e didattica.

Le applicazioni della piattaforma consentono di gestire in modo efficace il flusso informativo all'interno dell'Istituto attraverso tre strumenti principali e relative applicazioni:

- ✓ Comunicazione: posta elettronica, strumenti per la chat, strumenti di video lezione, gestione gruppi, calendario;
- ✓ Archiviazione: spazio in cloud;
- ✓ Collaborazione: condivisione di documenti, fogli, presentazioni, moduli, sites e di spazio online per la gestione di una classe virtuale.

Fermo restando quanto già sottoscritto nelle liberatorie in merito alla privacy, acquisite agli atti, e quanto contenuto nelle informative pubblicate sul sito web della scuola, con il presente atto si intende disciplinare il trattamento dei dati che scaturiscono dall'uso della piattaforma EDMODO, e/o di qualsiasi altro strumento la scuola adotterà, al fine e rendere più efficace la didattica a distanza.

Tali dati saranno trattati secondo i principi di liceità, correttezza e trasparenza, nel rispetto della vigente normativa europea e nazionale in materia di protezione dei dati personali (Regolamento UE 2016/679 e D. Lgs 196/2003 così come integrato e modificato dal D. Lgs 101/2018), nonché del Children's On line Privacy Protection Act del 1998.

1) Dati del Titolare e del Responsabile per la Protezione dei Dati (RPD)

Il Titolare del Trattamento, è il Dirigente Scolastico p.t., dott.ssa Ida Francioni , i cui dati di contatto sono esplicitati nell'intestazione della presente informativa.

I dati del Responsabile per la Protezione dei Dati, sono indicati nel sito:<https://www.scuolavarvitelli36.edu.it>

2) Natura dei dati personali trattati e modalità del trattamento

Il trattamento ha ad oggetto i dati anagrafici identificativi, e i dati di contatto (mail o ID di programmi di messaggistica) degli alunni iscritti, nonché quelli contenuti nei documenti creati e/o caricati attraverso i servizi delle piattaforme.

Il trattamento dei dati conferiti è realizzato con il supporto di mezzi cartacei e/o informatici e attraverso un complesso di operazioni quali la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, etc., necessarie per la realizzazione delle finalità.

Le modalità di trattamento includono:

- condivisione da parte del docente per via telematica agli alunni del gruppo classe di materiale didattico (file, documentazioni, etc.) e delle registrazioni audio/video delle lezioni;
- acquisizione per via telematica, da parte del docente, degli elaborati degli alunni;
- videoconferenza online attraverso piattaforme;

3) Finalità del trattamento dei dati personali

I dati personali forniti dagli utenti verranno utilizzati per l'assolvimento degli obblighi istituzionali della Scuola per la gestione delle attività di didattica a distanza, rientranti nel programma di studio ed in particolare:

- ✓ per aumentare la produttività didattica;
- ✓ per apprendere le competenze di cittadinanza digitale del XXI secolo;
- ✓ per creare, scambiare e condividere materiali didattici e disciplinari;
- ✓ per effettuare in sincrono una eventuale videoconferenza;
- ✓ per scrivere e ricevere posta elettronica all'interno dell'istituto;
- ✓ per organizzare una classe virtuale in cui assegnare, ricevere e correggere verifiche e/o compiti/lavori diversificati;
- ✓ per far condividere/creare a docenti e alunni materiali di studio, di ricerca e di lavoro direttamente in ambiente drive.

4) Base giuridica e Natura del conferimento

La base giuridica del trattamento dati è da ravvisarsi nell'esecuzione di un compito di interesse pubblico e connesso all'esercizio di pubblici poteri.

Il conferimento dei dati personali richiesti è facoltativo. Tuttavia il mancato conferimento degli stessi o il mancato consenso all'uso, comporta l'impossibilità di accedere ai servizi di didattica a distanza.

5) Comunicazione e diffusione dei dati personali e trasferimento verso un paese terzo

I dati personali conferiti, saranno comunicati alle piattaforme utilizzate per la gestione della “didattica a distanza” partner di formazione e di attività educative. A tal proposito si invitano gli utenti a prendere visione delle condizioni d’uso delle stesse.

Saranno comunicati altresì alle Autorità competenti, nelle ipotesi di accertamento del compimento di attività illecite.

Secondo le finalità sopra descritte, i dati personali specificamente conferiti dagli utenti potranno essere oggetto di trattamento da parte di collaboratori interni, nella loro qualità di incaricati.

I dati non sono soggetti a diffusione da parte dell’Istituto.

6) Durata del trattamento

Il trattamento da parte dell’Istituto avrà una durata non superiore a quella necessaria alle Finalità per le quali i dati personali sono stati raccolti. Tuttavia i dati saranno conservati secondo le indicazioni e le regole tecniche in materia di conservazione digitale degli atti definite da AGID e nei tempi e nei modi indicati dalle Linee Guida per le istituzioni scolastiche e dai Piani di conservazione e scarto degli archivi scolastici definiti dalla direzione Generale degli archivi presso il Ministero dei Beni Culturali.

7) Diritti dell’interessato

L’utente avrà in qualsiasi momento piena facoltà di esercitare i diritti previsti dalla normativa vigente, tra cui i seguenti diritti:

- ✓ ricevere conferma dell’esistenza dei suoi dati personali e richiedere l’accesso al loro contenuto;
- ✓ chiedere la cancellazione dell’account;
- ✓ revocare il consenso prestato;
- ✓ opporsi per motivi legittimi al trattamento e proporre reclamo.

Per esercitare uno o più dei diritti sopra elencati, è possibile inviare specifica richiesta al titolare presso la segreteria dell’Istituto oppure via e-mail all’indirizzo: naee03600t@istruzione.it

Per tutto quanto non espressamente indicato si rinvia all’informativa presente sul sito web della scuola

REGOLE DI UTILIZZO

Con la pubblicazione di tale informativa si intende che ogni genitore abbia recepito ed accetti tali regole anche ai sensi della normativa locale, nazionale ed europea vigente.

È solo in tal modo che l’alunno potrà usare le credenziali ricevute per accedere alla piattaforma scelta.

Pertanto si impegna a:

- ✓ a conservare la password personale e a non consentirne l’uso ad altri soggetti;
- ✓ a comunicare immediatamente attraverso mail al seguente indirizzo: naee03600t@istruzione.it l’impossibilità ad accedere al proprio account o il sospetto che altri possano accedervi;
- ✓ a non consentire ad altri, a nessun titolo, l’utilizzo della piattaforma EDMODO, o di qualsiasi altro programma venga usato, con le proprie credenziali;
- ✓ a non diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all’attività delle altre persone che utilizzano il servizio;
- ✓ a non registrare con nessun mezzo o strumento le lezioni online;

- ✓ ad osservare il presente regolamento, pena la sospensione alle attività da parte dell'Istituto dell'account personale dello Studente;
- ✓ ad utilizzare i servizi offerti solo ad uso esclusivo per le attività didattiche della scuola.

Le lezioni online costituiscono di fatto attività didattica dell'istituto "36°C.D. Luigi Vanvitelli" e in quanto tali ad esse possono partecipare solo gli alunni iscritti.

Gli alunni accedono alle lezioni online (sincrone) seguendo le indicazioni fornite dai singoli docenti, in modalità:

- lezioni asincrono mediante la piattaforma EDMODO
- video mediante strumenti e APP di video conferenza, **sotto la diretta supervisione dei genitori**, con sessioni organizzate e moderate dal docente della classe;
- audio mediante adeguati strumenti e APP, disabilitando la videocamera e lasciando attivo il solo microfono;
- chat testuale mediante strumenti e APP dedicati.

È **assolutamente vietato registrare con qualsiasi mezzo o strumento** le lezioni online; sarà il docente, se lo ritiene opportuno, registrare la lezione per renderla disponibile off-line all'interno della piattaforma EDMODO

È fatto divieto di condividere all'esterno della piattaforma scolastica le registrazioni pubblicate dai docenti.

È fatto, altresì, divieto di condivisione del "link alla lezione" con soggetti esterni alla Scuola.

Si ricorda che, i genitori/tutori, ai sensi dell'art.2048 c.c., sono responsabili di tutti i fatti illeciti derivanti dai comportamenti dei propri figli nell'uso di tali strumenti.

Limiti di Responsabilità

La scuola non si ritiene responsabile di eventuali danni arrecati allo Studente a causa di guasti e/o malfunzionamenti del servizio.

La Dirigente Scolastica

Dr.ssa Ida Francioni

Firma autografa omessa ai sensi art.3 D.Lgs 39/9



Coronavirus: Didattica on line, dal Garante privacy prime istruzioni per l'uso

VEDI ANCHE

[- Provvedimento del 26 marzo 2020 - "Didattica a distanza: prime indicazioni"](#)

[- Nota istituzionale del Presidente del Garante, Antonello Soro, alla Signora Ministro dell'Istruzione, al Signor Ministro dell'Università e della ricerca e alla Signora Ministro per le pari opportunità e la famiglia in tema di didattica a distanza](#)

Coronavirus: Didattica on line, dal Garante privacy [prime istruzioni per l'uso](#)

Nell'intento di fornire a scuole, atenei, studenti e famiglie [indicazioni utili](#) a un utilizzo quanto più consapevole e positivo delle nuove tecnologie a fini didattici, il Garante per la privacy ha approvato uno specifico atto di indirizzo che individua le implicazioni più importanti dell'attività formativa a distanza sul diritto alla protezione dei dati personali.

Nella lettera inviata al Ministro dell'Istruzione, al Ministro dell'Università e della ricerca e al Ministro per le pari opportunità e la famiglia per illustrare gli obiettivi del provvedimento, il presidente dell'Autorità Garante, Antonello Soro, ha ricordato che "il contesto emergenziale in cui versa il Paese ha imposto alle istituzioni scolastiche e universitarie, nonché alle famiglie stesse, l'esigenza di proseguire l'attività didattica con modalità innovative, ricorrendo alle innumerevoli risorse offerte dalle nuove tecnologie. È una soluzione estremamente importante per garantire la continuità didattica". E tuttavia, ha sottolineato Soro, "le straordinarie potenzialità del digitale - rivelatesi soprattutto in questo frangente indispensabili per consentire l'esercizio di diritti e libertà con modalità e forme nuove - non devono indurci a sottovalutare anche i rischi, suscettibili di derivare dal ricorso a un uso scorretto o poco consapevole degli strumenti telematici, spesso dovuto anche alla loro oggettiva complessità di funzionamento". "Considerando che, spesso, per i minori che accedono a tali piattaforme si tratta delle prime esperienze (se non addirittura della prima) di utilizzo di simili spazi virtuali, è evidente come anche quest'attività vada svolta con la dovuta consapevolezza, anche sulla base delle indicazioni fornite a livello centrale".

Da qui l'esigenza di assicurare al mondo della scuola e dell'università un supporto utile alla gestione della didattica on line.

Queste, in sintesi, le prime "istruzioni per l'uso" indicate del Garante.

Nessun bisogno di consenso

Le scuole e le università che utilizzano sistemi di didattica a distanza non devono richiedere il consenso al trattamento dei dati di docenti, alunni, studenti, genitori, poiché il trattamento è riconducibile alle funzioni istituzionalmente assegnate a scuole e atenei.

Scelta e regolamentazione degli strumenti di didattica a distanza

Nella scelta e nella regolamentazione degli strumenti più utili per la realizzazione della didattica a distanza scuole e università dovranno orientarsi verso strumenti che abbiano fin dalla progettazione e per impostazioni predefinite misure a protezione dei dati. Non è necessaria la valutazione di impatto, prevista dal Regolamento europeo per i casi di rischi elevati, se il trattamento dei dati effettuato dalle istituzioni scolastiche e universitarie, per quanto relativo a minorenni e a lavoratori, non presenta ulteriori caratteristiche suscettibili di aggravarne i rischi. Ad esempio, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola (non, quindi, su larga scala) nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una

piattaforma che non consente il monitoraggio sistematico degli utenti.

Ruolo dei fornitori dei servizi on line e delle piattaforme

Se la piattaforma prescelta comporta il trattamento di dati personali di studenti, alunni o dei rispettivi genitori per conto della scuola o dell'università, il rapporto con il fornitore dovrà essere regolato con contratto o altro atto giuridico. E' il caso, ad esempio, del registro elettronico, il cui fornitore tratta i dati per conto della scuola. Nel caso, invece, in cui si ritenga necessario ricorrere a piattaforme più complesse che erogano servizi più complessi anche non rivolti esclusivamente alla didattica, si dovranno attivare i soli servizi strettamente necessari alla formazione, configurandoli in modo da minimizzare i dati personali da trattare (evitando, ad esempio, geolocalizzazione e social login).

Le istituzioni scolastiche e universitarie dovranno assicurarsi che i dati trattati per loro conto siano utilizzati solo per la didattica a distanza.

L'Autorità vigilerà sull'operato dei fornitori delle principali piattaforme per la didattica a distanza, per assicurare che i dati di docenti, studenti e loro familiari siano trattati nel pieno rispetto della disciplina di protezione dati e delle indicazioni fornite dalle istituzioni scolastiche e universitarie.

Limitazione delle finalità del trattamento dei dati

Il trattamento di dati svolto dalle piattaforme per conto della scuola o dell'università dovrà limitarsi a quanto strettamente necessario alla fornitura dei servizi richiesti ai fini della didattica on line e non per ulteriori finalità proprie del fornitore.

I gestori delle piattaforme non potranno condizionare la fruizione di questi servizi alla sottoscrizione di un contratto o alla prestazione del consenso (da parte dello studente o dei genitori) al trattamento dei dati per la fornitura di ulteriori servizi on line, non collegati all'attività didattica.

Ai dati personali dei minori, inoltre, va garantita una specifica protezione poiché i minori possono essere meno consapevoli dei rischi, delle conseguenze e dei loro diritti. Tale specifica protezione deve, in particolare, riguardare l'utilizzo dei loro dati a fini di marketing o di profilazione.

Correttezza e trasparenza nell'uso dati

Per garantire la trasparenza e la correttezza del trattamento, le istituzioni scolastiche e universitarie devono informare gli interessati (alunni, studenti, genitori e docenti), con un linguaggio comprensibile anche ai minori, riguardo, in particolare, alle caratteristiche essenziali del trattamento che viene effettuato. Relativamente ai docenti, scuole e università, nel rispetto della disciplina sui controlli a distanza, dovranno trattare solo i dati strettamente necessari e comunque senza effettuare indagini sulla sfera privata.

Roma, 30 marzo 2020