IC PERNA ALIGHIERI - AVELLINO - Protocollo 0000597 del 17/01/2023

Ministero dell'Istruzione

Istituto Comprensivo Statale "Luigi Perna - Dante Alighieri"

Scuola Secondaria di primo grado ad Indirizzo musicale

1° premio nazionale al concorso: "M9 Urban Contest Landscape"
1° premio nazionale al concorso: "Fellini in Craft"
1° premio nazionale al concorso: "Carmine Sciangueta"
2° classificato al Premio Smart School 2021

Prot. n. (vedi segnatura) Avellino, 17.01.2023

POLICY E-SAFETY
- Sicurezza in rete-

A.S. 2022/23

Generazioni Connesse
SAFER INTERNET CENTRE

Co-financed by the European Union
Connecting Europe Facility

Sommario

1. INTRODUZIONE E PROCESSO DI REVISIONE 3
2. SCOPO DELLA POLICY DI E-SAFETY 3
3. STATO DI FATTO: SPAZI FISICI E VIRTUALI DISPONIBILI NELLA SCUOLA 4
4. STRATEGIE DELLA SCUOLA PER GARANTIRE LA SICUREZZA DELLE TIC 5
5. LINEE GUIDA DI BUONA CONDOTTA DEGLI UTENTI 6
5.1 DOCENTI 7
5.2 STUDENTI 9
5.3 GENITORI 10
6. ALTRE TIPOLOGIE DI TIC 10
7. LA NETIQUETTE 11
8. COMUNICAZIONE SCUOLA-FAMIGLIA 12
9. GARANZIA E TUTELA DELLA PRIVACY 13
10. DIDATTICA E AZIONE DEI DOCENTI 14
11. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI 16
11.1 Prevenzione 16
11.2 Rilevazione e gestione dei casi 16
GLOSSARIO 18

1. INTRODUZIONE E PROCESSO DI REVISIONE

L'Istituto Comprensivo L.Perna-D.Alighieri ha ritenuto opportuno dotarsi di una policy di e-safety per essere pronto a cogliere i cambiamenti in atto nell'attuale società della conoscenza in cui opera, in particolare per quanto riguarda la formazione dei cittadini del futuro, destinatati a vivere in un ambiente in cui tutto viene gestito attraverso l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC). Tali tecnologie diventano abilitanti, quotidiane, ordinarie, al servizio dell'attività scolastica e di tutti i suoi ambienti, coinvolgendo sia le attività orientate alla formazione e all'apprendimento sia l'amministrazione, con ricadute estese al territorio.

Con questo documento si vuole regolamentare l'uso di Internet per rendere responsabili tutti gli utenti dell'Istituto in modo tale da garantire la privacy all'interno dei plessi e degli uffici di segreteria. Le indicazioni nazionali pongono l'accento sulle competenze digitali degli studenti, ai quali è richiesto di sapersi orientare nelle molteplici possibilità offerte dal Web, analizzando criticamente i materiali disponibili, scambiando informazioni ed esperienze in modo consapevole e responsabile. Occorre in tal senso informare e formare le componenti scolastiche, in particolare gli alunni, in merito a eventuali rischi e fornire misure atte a prevenirli, permettendo di beneficiare in sicurezza delle opportunità offerte da Internet e dalle TIC.

Al termine del documento è inserito un glossario per una migliore comprensione.

La policy di e-safety verrà revisionata e aggiornata periodicamente in base a eventuali variazioni delle norme, delle dotazioni tecnologiche e dei protocolli dell'Istituto.

2. SCOPO DELLA POLICY DI E-SAFETY

Scopo del presente documento è quello di informare l'utenza al fine di garantire un uso corretto e responsabile delle apparecchiature informatiche in dotazione alla scuola, nel rispetto della normativa vigente. È pertanto fondamentale conoscere le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico, le misure per la prevenzione e quelle per la rilevazione e la gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.

Tutti gli utenti devono conoscere i rischi cui sono esposti ogni volta che navigano in Internet: esiste, infatti, la possibilità che durante il lavoro online si possa entrare accidentalmente

in contatto con materiale inadeguato e/o illegale. L'Istituto, pertanto, promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.

In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, al fine di prevenire il verificarsi di situazioni potenzialmente pericolose. I docenti, consapevoli che è impossibile garantire una navigazione totalmente priva di rischi negli ambienti scolastici, non possono assumersi responsabilità derivanti da accessi accidentali e/o impropri a siti illeciti o dal reperimento e uso di materiali inappropriati.

3. STATO DI FATTO: SPAZI FISICI E VIRTUALI DISPONIBILI NELLA SCUOLA

Nell'Istituto la qualità e la quantità degli strumenti è in continua implementazione:

- la dotazione di nuovi strumenti informatici è un obiettivo prioritario, a partire dalla presenza della LIM in tutte le classi dell'istituto
- l'implementazione del cablaggio in alcuni plessi dell'Istituto è avvenuto tramite la partecipazione al PON 13.1.1A-FESRPON-CA-2021-470 "Cablaggio strutturato e sicuro all'interno degli edifici scolastici"";
- il registro elettronico è in uso nei tre ordini di scuola;
- i laboratori di informatica, presenti nei vari plessi, sono dotati di connessione Internet attraverso rete WIFI e cavo, postazioni PC per alunni e videoproiettore;
- la segreteria, seguendo la normativa vigente, sta progressivamente raggiungendo l'obiettivo della completa dematerializzazione; si presta particolare attenzione al potenziamento delle attrezzature informatiche, al mantenimento e al costante aggiornamento della rete informatica, al potenziamento dei servizi digitali scuola-famiglia-studente.

I referenti dei diversi laboratori hanno il compito di verificarne il funzionamento e il rispetto del regolamento.

Gli insegnanti e il personale ATA sono tenuti a utilizzare con il massimo rispetto gli strumenti presenti nella scuola, seguendo i regolamenti vigenti e minimizzando gli sprechi delle risorse a disposizione.

I docenti devono servirsi con criterio delle TIC nelle attività didattiche e hanno il fondamentale compito di responsabilizzare gli studenti, per renderli consapevoli dell'importanza della salvaguardia di un bene comune, mediante corrette norme di utilizzo.

4. STRATEGIE DELLA SCUOLA PER GARANTIRE LA SICUREZZA DELLE TIC

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

- analizzare il fabbisogno formativo dei docenti e promuovere corsi di formazione inerenti all'uso sicuro e responsabile delle TIC e del Web, sia nel loro uso privato, sia a scuola;
- attuare, eventualmente in collaborazione con esperti esterni, incontri per presentare a tutte le componenti della comunità scolastica:
- modalità corrette di fruizione del Web;
- tutela dei minori su Internet e sui social network;
- prevenzione e contrasto del fenomeno del cyberbullismo e dell'uso responsabile del web;
- informare sulle problematiche psico-pedagogiche correlate all'uso della Rete;
- organizzare le reti dei plessi in sotto reti dedicate a differenti tipologie di utenti;
- creare profili per diverse tipologie d'utenza;
- monitorare periodicamente il sistema informatico, in particolare per ciò che concerne l'uso di Internet, cronologia, cookie…, a cura dei responsabili dei laboratori avvisando preventivamente gli utenti del controllo;
- chiedere, al bisogno, l'intervento delle società informatiche che si occupano di manutenzione e assistenza dei dispositivi con azioni in loco o da remoto;

- garantire la costante presenza di un docente durante l'utilizzo di Internet o di altre TIC;
- installare firewall sull'accesso a Internet;
- aggiornare con regolarità il sistema operativo, i software applicativi e l'antivirus; scansionare i dispositivi in cui si può sospettare la presenza di virus o malware;
- utilizzare penne USB, CD, DVD o altri dispositivi esterni personali solo se preventivamente autorizzati dal docente responsabile;
- organizzare un sistema di monitoraggio di eventuali problemi riscontrati durante l'uso delle TIC o della Rete e prevedere piani d'azione per risolvere i più frequenti;
- evidenziare il divieto di adottare comportamenti contrari al presente regolamento e alla normativa vigente come, ad esempio,
    a. scaricare file protetti da copyright e violare le leggi sui diritti d'autore;
    b. visitare siti non inerenti all'attività didattica, usare la Rete per interessi privati e personali;
    c. alterare i parametri di protezione dei dispositivi utilizzati.

5. LINEE GUIDA DI BUONA CONDOTTA DEGLI UTENTI

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

- rispettare il presente regolamento e la legislazione vigente;
- tutelare la propria privacy, quella degli alunni e quella degli altri utenti adulti al fine di non divulgare notizie private contenute nelle documentazioni digitali cui ha accesso;
- rispettare la netiquette, ossia le regole condivise che disciplinano il rapportarsi tra utenti della Rete, in contatto attraverso siti, forum, mail, blog, newsgroup…

Si indicano i comportamenti da tenere rispettivamente riferite ad attività e a utenti.

5.1 DOCENTI

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

- leggere, comprendere e aderire a questa policy;
- aver cura degli strumenti in dotazione, in particolare spegnendo correttamente tablet, PC, LIM e videoproiettori al termine del periodo di utilizzo collocandoli nel luogo predisposto;
- il docente dell'ultima ora di lezione è tenuto a verificare che tutti gli strumenti siano correttamente spenti e riposti;
- accedere personalmente al registro elettronico attraverso il tablet o dal pc in uso e provvedere a compilare quanto di competenza; il tablet o il pc devono essere custoditi, tenuti fuori dalla portata degli alunni; sarà cura del docente non lasciare incustoditi i dispositivi in uso negli spostamenti della classe in altri luoghi della scuola;
- custodire la segretezza delle credenziali d'accesso al registro elettronico e all'area riservata del sito della scuola;
- non divulgare agli alunni le credenziali di accesso alla rete WIFI riservata ai docenti;
- installare e utilizzare solo software autorizzati;
- lasciare invariate le impostazioni dei dispositivi della scuola;
- compilare il registro d'uso per garantire la tracciabilità delle attività e il mantenimento in buono stato della strumentazione tecnologica utilizzata, segnalando celermente eventuali malfunzionamenti ai responsabili, secondo le modalità previste;
- non salvare sui dispositivi utilizzati file contenenti dati personali e/o sensibili;

- non memorizzare credenziali, email, file personali sui dispositivi;
- assicurarsi di aver effettuato il logout da ogni servizio prima di lasciare la postazione;
- salvare file di lavoro in cartelle personali o di classe e non sul desktop; i file non salvati in tal modo saranno eliminati dal responsabile delle attrezzature;
- utilizzare il laboratorio attenendosi all'orario concordato a inizio anno, firmare il registro d'accesso compilando i campi richiesti, segnalare eventuali malfunzionamenti riscontrati prima, durante o alla conclusione dell'attività svolta;
- permettere l'accesso al laboratorio agli alunni solo se accompagnati da docenti;
- prima di lasciare il laboratorio, accertarsi che tutti i pc siano stati spenti nel modo corretto; se necessario, compilare il modulo per la segnalazione di problemi;
- controllare l'uso corretto del laboratorio e della strumentazione, assicurandosi che non vengano introdotti cibi o bevande;
- applicare le medesime precauzioni nelle aule aumentate dalla tecnologia;
- illustrare agli alunni il presente documento e informarli delle eventuali sanzioni disciplinari previste dal Regolamento di Istituto;
- premurarsi che l'accesso degli alunni alla Rete avvenga sempre sotto la propria supervisione, informarli sui rischi cui sono potenzialmente esposti e sul corretto uso della Rete (motori di ricerca, piattaforme online, classi virtuali);
- visionare preventivamente i siti da proporre, verificandone accuratamente la sicurezza e il rispetto dei diritti di proprietà intellettuale;
- guidare gli alunni nelle ricerche online: fornire obiettivi chiari, proporre indirizzi web, parole chiave per la ricerca, prediligendo siti istituzionali, creati ad hoc per la didattica; vigilare, durante la navigazione, che tutti usino in modo corretto la Rete, fornendo costanti indicazioni su ciò che è richiesto dalla netiquette;

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

5.2 STUDENTI

Durante l'attività didattica gli alunni devono:

- leggere, comprendere e aderire a questa policy;
- accedere al laboratorio di informatica solo se accompagnati da docenti e seguire le indicazioni fornite in merito all'utilizzo delle TIC;
- accedere agli ambienti di lavoro con le proprie credenziali, senza divulgarle, e archiviare i propri file in modo ordinato, così da essere facilmente rintracciabili, all'interno di cartelle dedicate o su supporto esterno preventivamente autorizzato;
- accedere alla Rete solo in presenza e previa autorizzazione del docente responsabile dell'attività;
- utilizzare la strumentazione della scuola solo per scopi didattici e non personali;
- lasciare immutata la configurazione di sistema dei dispositivi;
- chiudere correttamente la propria sessione di lavoro.

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

Inoltre per specifiche attività didattiche organizzate dal docente di classe è consentito l'uso a scuola di dispositivi personali (BYOD). In tutte le attività didattiche che comportano l'uso delle nuove tecnologie e di dispositivi personali, sia a scuola, sia durante i viaggi di istruzione, si applicano le misure sopra citate.

5.3 GENITORI

I genitori sono tenuti a

- leggere, comprendere e promuovere la policy di e-safety con i loro figli;
- controllare con regolarità il registro elettronico e il sito istituzionale dell'Istituto;
- monitorare il modo in cui i figli usano la tecnologia e guidarli verso un comportamento responsabile e sicuro;
- collaborare con la scuola per la realizzazione di attività e progetti che prevedono l'utilizzo di dispositivi personali (BYOD);
- confrontarsi con i docenti e/o dirigente scolastico dell'Istituto se dovessero sorgere preoccupazioni riguardo l'uso delle nuove tecnologie da parte del figlio.

6. ALTRE TIPOLOGIE DI TIC

Lo studente non può utilizzare per scopi personali i device di sua proprietà nei locali scolastici e relative pertinenze; l'eventuale utilizzo durante una specifica attività didattica, inserita nel PTOF, deve essere autorizzata e costantemente supervisionata dal docente di classe. Durante l'orario scolastico, agli studenti non è permesso l'uso della telefonia mobile.

Le infrazioni e le sanzioni relative a un uso improprio delle TIC da parte degli studenti sono declinate nel Regolamento d'Istituto.

7. LA NETIQUETTE

Chiunque si trovi a utilizzare le TIC, Internet e i servizi offerti dalla Rete, deve attenersi a una serie di regole che disciplinano il comportamento degli utenti nel rapportarsi con gli altri. Tali norme costituiscono la cosiddetta netiquette, una sorta di galateo della Rete.

Si riportano alcune delle norme su cui si intende sensibilizzare in modo particolare l'utenza:

- in Rete la comunicazione avviene principalmente attraverso testi, con conseguente rischio di essere fraintesi; talvolta, nei contesti opportuni, le emoticon possono anche aiutare a chiarire il tono del messaggio;
- evitare di inviare messaggi ripetitivi, inutili o inopportuni (spam); evitare altresì l'invio di messaggi pubblicitari, catene o comunicazioni non espressamente richieste;
- in Rete si possono esprimere la propria opinione e le proprie idee, sempre rispettando tutti gli interlocutori e i fruitori del messaggio; la Rete offre la possibilità di entrare in contatto con milioni di utenti, dei quali vanno rispettati la nazionalità, la cultura, la religione, il sesso; non sono ammessi forme di insulto, minaccia, razzismo o discriminazione;
- è necessario rispettare gli interlocutori virtuali: i loro tempi nella risposta, che non andrà mai pretesa, il loro interesse o meno a quanto proposto; gli errori di digitazione, di grammatica o di sintassi non devono essere stigmatizzati, l'importante è che la trasmissione del messaggio avvenga con successo; si ricorda che lo scrivere in maiuscolo equivale a urlare: non abusarne;
- scegliere forum, social, community, chat, mailing list… cui si intende partecipare in base agli argomenti che interessano o alle esigenze emerse; partecipare rispettandone le regole e gli interventi dei moderatori;

- l'espressione del proprio parere deve avvenire in modo pacato, così da non provocare dure reazioni nelle persone con cui si comunica;
- non utilizzare le proprie competenze digitali per violare siti o profili di altri utenti, pubblicare contenuti o conversazioni private, condividere fotografie, video o altri file di utenti terzi senza averne il consenso;
- curare la propria reputazione digitale, valutando sempre con la massima attenzione ciò che si vuole comunicare, pubblicare e condividere;
- rispettare la privacy degli altri utenti: ognuno può scegliere cosa pubblicare e cosa condividere delle informazioni che lo riguardano;
- evitare di rivelare dettagli, informazioni personali o dati sensibili propri o altrui;
- utilizzare la Rete con spirito critico: evitare di credere a tutto ciò che viene detto e diffidare di chi chiede informazioni personali o incontri dopo poco tempo che si è entrati in contatto perché non sempre è possibile avere la certezza dell'identità della persona con la quale si sta comunicando.

8. COMUNICAZIONE SCUOLA-FAMIGLIA

L'Istituto si impegna a promuovere una comunicazione chiara ed esplicita con il personale, le famiglie e il territorio, in particolare attraverso

- il sito istituzionale, costantemente aggiornato, che fornisce un'informazione puntuale e trasparente sulla documentazione e le attività relative alla scuola;
- il registro elettronico, costantemente aggiornato dai docenti, sul quale le famiglie possono controllare assenze, voti e annotazioni;

- la posta elettronica istituzionale, canale preferenziale per la trasmissione di informazioni e comunicazioni tra gli utenti.

L'Istituto fornisce un supporto alle famiglie per le iscrizioni online mediante postazioni informatiche dedicate e personale applicato di segreteria.

L'Istituto, conseguentemente alla dematerializzazione, sta valutando di dotarsi di un sistema per la firma grafometrica, predisposto per tutti gli utenti.

9. GARANZIA E TUTELA DELLA PRIVACY

L'Istituto opera a ogni livello rispettando tutte le normative vigenti in merito alla tutela della privacy, come indicato sul sito istituzionale.

La compilazione della liberatoria riguardante il trattamento immagini e audiovisivi degli alunni è richiesta

- a chi si iscrive per la prima volta nell'Istituto attraverso la compilazione del modulo di iscrizione;
- a ciascun alunno all'inizio di ogni anno scolastico attraverso l'apposita modulistica presente sul sito istituzionale.

Sono permesse a titolo gratuito le riprese video e fotografiche di visite o viaggi di istruzione, saggi e rappresentazioni scolastiche se destinate a un ambito familiare e non alla diffusione. Deve essere prestata grande attenzione all'eventuale pubblicazione delle medesime immagini in internet e, in particolare, sui social network per i quali è indispensabile il consenso informato delle persone presenti nel video e nelle immagini/fotografie, se minorenni, dei rispettivi genitori.

10. DIDATTICA E AZIONE DEI DOCENTI

L'Istituto, come evidenziato nel Piano Triennale dell'Offerta Formativa, pone particolare attenzione allo sviluppo della competenza digitale dei propri studenti, in linea con quanto previsto dal Piano Nazionale per la Scuola Digitale (PNSD). Questa competenza non può prescindere da quelle sociali e civiche, soprattutto per gli aspetti relazionali da esse implicati. In tal modo ci si prefigge di prevenire eventuali fenomeni di disagio giovanile.

La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni, nonché per comunicare e partecipare a reti collaborative tramite Internet. Si pone al centro dell'attenzione educativa la capacità di esplorare e affrontare in modo flessibile situazioni tecnologicamente nuove, adeguando le performance ai diversi contesti in cui si opera, in modo tale da:

- analizzare e valutare criticamente i dati e le informazioni con cui ci si confronta durante la navigazione online e l'uso delle TIC;
- sfruttare le potenzialità offerte dalle TIC per la risoluzione di problemi;
- costruire e condividere le conoscenze acquisite, sviluppando una consapevole responsabilità in merito ai dati personali e alla tutela della privacy, con particolare attenzione ai diritti e doveri reciproci degli utenti.

La competenza digitale è interazione tra:

- **etica,** inerente alla responsabilità sociale, al sapere relazionarsi con gli altri utenti, al tenere dei comportamenti adeguati alle circostanze in cui ci si può imbattere e alla tutela della propria persona, per preservare la quale è necessario sapersi schermare dai possibili rischi;
- **tecnologia,** saper individuare gli usi e i punti di forza dei dispositivi in uso e, quindi, scegliere i device e i mezzi adeguati per risolvere problemi;
- **conoscenze**, grazie alle quali è possibile saper leggere, selezionare e valutare dati, attraverso modelli astratti che conducano a un'analisi critica degli stessi.

Per perseguire questi traguardi, i docenti adottano, come supporto alle attività scolastiche, le tecnologie educative e didattiche a disposizione, quali LIM, digital board, libri di testo digitali, risorse multimediali.

I media sono visti come un supporto fondamentale per un apprendimento disciplinare efficace. Ai docenti spetta il compito di promuovere una riflessione critica e una sperimentazione creativa, approfondendo le dinamiche che regolano il sistema dei media stessi, la decodifica dei messaggi e la conoscenza dei linguaggi e di nuovi metodi e strategie didattiche.

L'Istituto in epigrafe, coerentemente con quanto previsto dal PNSD, attiva dei percorsi di formazione rivolti ai docenti per incrementare le loro competenze digitali.

11. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

11.1 Prevenzione

L'Istituto si prefigge come obiettivo quello di fornire all'utenza le competenze necessarie al fine di tenere comportamenti responsabili e corretti per un uso corretto e responsabile nella fruizione delle TIC e della Rete.

Fondamentale è anche diffondere le nozioni per una navigazione sicura, corretta e responsabile come precedentemente indicato nel paragrafo "Strategie dell'Istituto per garantire la sicurezza delle TIC".

11.2 Rilevazione e gestione dei casi

L'Istituto si impegna a formare e aggiornare i docenti sulle modalità, sugli indicatori per riconoscere eventuali casi di cyberbullismo o situazioni a rischio e in merito alle procedure da seguire. Per i casi di bullismo o cyberbullismo, l'Istituto si prodiga nella tutela dei minori coinvolti, senza renderli in alcun modo identificabili, con dati o altri strumenti.

Chiunque entri in possesso di dati certi ha la possibilità di denunciarli in forma tutelata.

Nel momento in cui si è a conoscenza di situazioni di cyberbullismo

- il docente avvisa immediatamente il Dirigente scolastico;
- il docente redige una relazione sull'accaduto;
- il Dirigente scolastico convoca, separatamente, le famiglie degli alunni coinvolti per informarle dell'accaduto e mette in atto le procedure previste dal Regolamento d'Istituto.

Si ricorda che, in caso di necessità ci si può rivolgere ai servizi di supporto appositamente attivi a livello nazionale.

Per segnalare contenuti inopportuni visionati sui media si può far riferimento al sito del CoReCom (Comitato Regionale per le Comunicazioni) all'indirizzo http://www.corecomlombardia.it/opencms/index.html.

La Polizia Postale e delle Comunicazioni https://www.commissariatodips.it/ è attualmente impegnata in attività a sostegno della navigazione protetta dei minori ed è competente a ricevere segnalazioni in merito a qualsiasi tipo di reato informatico.

Materiali informativi tratti da "La scuola a prova di privacy

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5601934

Si allega **GLOSSARIO**

IL DIRIGENTE SCOLASTICO
prof.ssa Amalia Carbone
(Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3, co. 2, D.L. vo 39/1993)

GLOSSARIO

da Generazioni connesse

http://www.generazioniconnesse.it/site/it/glossario/

ADESCAMENTO ONLINE o GROOMING
Il grooming (dall'inglese "groom" - curare, prendersi cura) rappresenta 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. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano gli strumenti (chat, SMS, social network, ecc) messi a disposizione dalla Rete (ma anche dai cellulari) per entrare in contatto con loro. Il grooming definisce il percorso attraverso il quale gradualmente l'adulto instaura una relazione - che deve connotarsi come sessualizzata - con il/la bambino/a o adolescente.

CYBERBULLISMO
Il cyberbullismo (detto anche "bullismo elettronico") è una forma di prepotenza virtuale attuata attraverso l'uso di internet e delle tecnologie digitali. Come il bullismo tradizionale è una forma di prevaricazione e di oppressione reiterata nel tempo, perpetrata da una persona o da un gruppo di persone più potenti nei confronti di un'altra percepita come più debole.

DEVICE
Dispositivi e apparecchi ad alta tecnologia e di piccole dimensioni (smartphone, e-book reader, tablet, PC, ecc.)

LIM
La Lavagna Interattiva Multimediale, detta anche LIM o lavagna elettronica, è una superficie interattiva su cui è possibile scrivere, disegnare, allegare immagini, visualizzare testi, riprodurre video o animazioni. I contenuti visualizzati ed elaborati sulla lavagna potranno essere quindi digitalizzati grazie a un software di presentazione appositamente dedicato.
La LIM è uno strumento di integrazione con la didattica d'aula poiché coniuga la forza della visualizzazione e della presentazione tipiche della lavagna tradizionale con le opportunità del digitale e della multimedialità.

MISURE DI SICUREZZA
Sono tutti gli accorgimenti tecnici ed organizzativi, i dispositivi elettronici o i programmi informatici utilizzati per garantire: che i dati non vadano distrutti o persi anche in modo accidentale, che solo le persone autorizzate possano accedervi, che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati sono stati raccolti.

MOTORE DI RICERCA
Un motore di ricerca è un programma che, in base a determinate parole chiave inserite da chi effettua la ricerca, analizza un insieme di dati e restituisce un indice dei contenuti disponibili, classificandoli in modo automatico in base a formule statistico-matematiche che ne indichino il grado di rilevanza, data una determinata chiave di ricerca.

OFFLINE
Indica lo stato in cui un computer o qualsiasi altro dispositivo informatico non è connesso ad Internet (o più in generale ad un sistema telematico).

ONLINE
Indica lo stato in cui un computer o qualsiasi altro dispositivo informatico è effettivamente collegato ad Internet e può navigare il www o scaricare messaggi.

POLICY DI E-SAFETY
La policy di e-safety è un documento che verrà autoprodotto dalla scuola, sulla base dell'indice ragionato messo a disposizione nella piattaforma online, volto a descrivere: la visione del fenomeno, le norme comportamentali e le procedure per l'utilizzo delle TIC in ambiente scolastico, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

RISCHI ONLINE
I rischi online rappresentano tutte quelle situazioni di pericolo e problematiche derivanti da un uso non consapevole e responsabile delle tecnologie digitali da parte di bambini/e, ragazzi e ragazze. Di seguito un elenco:

- Adescamento Online
- Cyberbullismo
- Sexting
- Violazione della Privacy
- Pornografia (recenti ricerche hanno sottolineato come la maggior parte degli adolescenti reperisca in Rete informazioni inerenti la sessualità, col rischio, spesso effettivo, del diffondersi di informazioni scorrette e/o l'avvalorarsi di falsi miti).
- Pedopornografia (con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone minorenni).

- Gioco d'azzardo o Gambling (giocare d'azzardo significa "puntare o scommettere una data somma di denaro, o oggetto di valore, sull'esito di un gioco che può implicare la dimostrazione di determinate abilità o basarsi sul caso").
- Dipendenza da Internet (Internet Addiction – i/le ragazzi/e che ne soffrono sono spesso inconsapevoli ma, lontani dalla Rete, manifestano presto insofferenza, irascibilità e altri sintomi di disagio).
- Videogiochi Online (alcuni rischi associati possono essere ad esempio: contatti impropri con adulti, contenuti violenti e/o inadeguati; acquisti incontrollati, ecc.).
- Esposizione a contenuti dannosi o inadeguati (es. contenuti razzisti, che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, ecc.).
- Dipendenza da shopping online (es. acquisti incontrollati, uso della carta di credito dei genitori a loro insaputa, ecc).

RISORSE (didattiche) DIGITALI
Per risorsa didattica digitale si intende qualsiasi fonte di natura digitale a supporto della didattica. Si va dall'uso dell'immagine digitalizzata ad un percorso didattico completo. In particolar modo, facciamo qui riferimento a strumenti per la progettazione, sviluppo, utilizzazione, gestione e valutazione di processi e risorse per l'insegnamento e l'apprendimento.

SETTORE EDUCATIONAL
Settore che lavora nell'ambito dell'educazione con finalità didattiche, di istruzione o formazione.

SEXTING
Il sexting (parola sincratica che unisce i termini inglesi sex e texting) rappresenta la pratica di inviare o postare messaggi di testo (SMS, ma anche tramite whatsapp e chat) e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet.

SOCIAL NETWORK
I Social Network sono siti internet che rendono possibile la creazione di una rete sociale virtuale e consentono agli utenti di condividere contenuti testuali, immagini, video e audio e di interagire tra loro.

Per entrare a far parte di un social network è necessario creare un proprio profilo personale, inserendo informazioni di contatto, ma anche interessi personali, amicizie ed esperienze di lavoro passate. È possibile poi allargare la propria rete sociale invitando gli amici e i collaboratori a farne parte, e cercare nella Rete persone con interessi affini o con le competenze necessarie per risolvere un certo problema, e condividere con queste persone qualsiasi tipo di informazione. Diventa quindi possibile costituire delle community tematiche in base alle proprie passione e aree di business, aggregando ad esse altri utenti e stringendo contatti di amicizia ed affari.

Esistono numerosi Social Network, tra i più popolari Facebook (con oltre 1 miliardo di profili attivi è il social network più grande al mondo), seguito da Twitter, Google+ e LinkedIn (SN che si occupa delle reti di contatti professionali), ecc.

TABLET
Il tablet è un computer portatile di dimensioni ridotte, sul cui schermo è possibile scrivere o impartire comandi col tocco delle dita o mediante un apposito stilo.

TECNOLOGIE DIGITALI o TIC
TIC è l'acronimo di Tecnologie dell'Informazione e della Comunicazione.
Con uso delle TIC nella didattica intendiamo l'utilizzo delle tecnologie informatiche e della comunicazione a supporto dei processi di apprendimento, indipendentemente dal fatto che le stesse siano state pensate e progettate per usi dichiaratamente didattici. Ad esempio: il blog non nasce come strumento didattico, ma oggi se ne fa uso nelle attività educative.

WI-FI
Sistema di comunicazione ad onde di frequenza radio che consente di collegare computer e relative periferiche in una rete locale senza utilizzare cavi; tale rete a sua volta può essere allacciata ad Internet tramite un router, permettendo di usufruire di tutti i servizi offerti dalla connettività.

AUTORIZZAZIONE
È il provvedimento adottato dal Garante della privacy con cui il titolare del trattamento in ambito privato (ad esempio la scuola) viene autorizzato a trattare determinati dati "sensibili" o giudiziari, oppure a trasferire dati personali all'estero. In materia di dati sensibili e giudiziari, il Garante ha emanato alcune autorizzazioni generali che consentono a varie categorie di titolari di trattare dati per gli scopi specificati senza dover chiedere singolarmente un'apposita autorizzazione al Garante.

CONSENSO
Nell'ambito della privacy è la libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (vedi TITOLARE). È sufficiente che il consenso sia "documentato" in forma scritta (ossia annotato, trascritto, riportato dal titolare o dal responsabile o da un incaricato del trattamento su un registro o un atto o un verbale), a meno che il trattamento riguardi dati "sensibili"; in questo caso occorre il consenso rilasciato per iscritto dall'interessato (ad esempio con la sua sottoscrizione).

DATO PERSONALE
Qualsiasi informazione che riguardi persone fisiche (come uno studente o un professore) identificate o che possono essere comunque identificate tramite ulteriori dati, quali un numero o un codice identificativo (ad esempio il

cosiddetto "codice studente"). Sono, tra gli altri, dati personali: il nome e cognome, l'indirizzo di residenza, il codice fiscale, la fotografia di una persona o la registrazione della sua voce, l'impronta digitale o i dati sanitari.

DATO SENSIBILE
Qualunque dato che può rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'appartenenza a partiti, sindacati o ad associazioni, lo stato di salute e la vita sessuale.

DIFFUSIONE
In ambito di privacy è l'atto di divulgare dati personali al pubblico o, comunque, a un numero indeterminato di soggetti in qualunque forma (ad esempio pubblicandoli su Internet), anche mediante la loro messa a disposizione o consultazione.

INCARICATO DEL TRATTAMENTO
In ambito di privacy è il dipendente (un professore, un componente della segreteria, etc.) o il collaboratore che per conto del titolare del trattamento dei dati (ad esempio il Ministero dell'Istruzione e del Merito) elabora o utilizza materialmente i dati personali sulla base delle istruzioni ricevute dal titolare medesimo (e/o dal responsabile, se designato).

INFORMATIVA
Contiene le informazioni che il titolare del trattamento deve fornire all'interessato per chiarire, in particolare, se quest'ultimo è obbligato o meno a rilasciare i dati, quali sono gli scopi e le modalità del trattamento, l'ambito di circolazione dei dati e in che modo si possono esercitare i diritti riconosciuti dalla legge.

INTERESSATO
La persona cui si riferiscono i dati personali (ad esempio lo studente o il professore).

PRIVACY
La privacy è il diritto alla riservatezza della propria vita privata e al controllo dei propri dati personali.
A dichiararlo è il codice privacy ex Decreto Legislativo n. 196/2003, "Codice in materia di protezione dei dati personali" la cui finalità è garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, della dignità dell'interessato (con riferimento alla riservatezza), dell'identità personale e del diritto di protezione dei dati personali. Il concetto di privacy è dunque correlato a quello di dato personale, che rappresenta ogni informazione che sia relativa all'identità della persona, attraverso la quale è identificata o identificabile.

RESPONSABILE DEL TRATTAMENTO

La persona, la società, l'ente, l'associazione o l'organismo cui il titolare può affidare (previa apposita designazione), anche all'esterno, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati.

RECLAMO
Il reclamo al Garante è un atto circostanziato con il quale si rappresenta all'Autorità una violazione della disciplina rilevante in materia di protezione dei dati personali. Al reclamo segue un eventuale procedimento amministrativo all'esito del quale possono essere adottati vari provvedimenti.

RICORSO
Il ricorso va presentato al Garante per far valere i diritti di cui all'articolo 7 del Codice della privacy solo quando la risposta del titolare (o del responsabile, se designato) all'istanza con cui si esercita uno o più dei predetti diritti non è pervenuta o viene ritenuta non soddisfacente. In alternativa al ricorso al Garante, l'interessato può rivolgersi all'Autorità giudiziaria ordinaria.

SEGNALAZIONE
Quando non è possibile presentare un reclamo circostanziato (in quanto, ad esempio, non si dispone di tutte le notizie necessarie) si può inviare al Garante una segnalazione, fornendo elementi utili a controllare l'applicazione della disciplina rilevante in materia di protezione dei dati personali.

TITOLARE DEL TRATTAMENTO
La persona fisica, l'impresa, la pubblica amministrazione, l'associazione, etc. cui fa capo effettivamente il trattamento di dati personali e alla quale spetta assumere le decisioni fondamentali sugli scopi e sulle modalità del trattamento medesimo (comprese le misure di sicurezza). In ambito scolastico, il titolare del trattamento in genere è il Ministero dell'Istruzione, dell'Università e della Ricerca, o l'istituto scolastico di riferimento.

TRATTAMENTO
Qualsiasi operazione (raccolta, archiviazione, utilizzo, consultazione, aggiornamento, cancellazione) che può essere effettuata utilizzando i dati personali degli studenti, dei professori o di altre persone.