Istituto Comprensivo Mezzolombardo - Paganella

PUA d'Istituto

Politica d'Uso Accettabile e Sicuro della rete

29 giugno 2021

Redatto a cura dell'animatore e del team digitale d'Istituto.

Approvato dal Collegio dei Docenti il 29-06-2021

Assunto dal Consiglio di Istituto il 02-07-2021

CONTENUTI

Introduzione

I nostri ragazzi vivono nel mondo della tecnologia.

Frequentemente vengono definiti “nativi digitali”, una generazione che vede il mondo tecnologico come qualcosa di naturale, perché l’hanno sperimentato e vissuto fin dalla più tenera età.

In base a questa definizione, talvolta criticata e fin troppo stereotipata, sarebbero in grado di sviluppare una maggiore dimestichezza nell’utilizzo dei dispositivi. A tal proposito, alcuni dubbi potrebbero sorgere: come facciamo noi adulti ad aiutarli nel processo di sviluppo delle loro capacità? Siamo in grado di traghettarli nel mare della condivisione virtuale? Conosciamo i rischi che si nascondono nella rete?

Il documento che segue cerca di dare risposte in merito, delineando alcune indicazioni per un corretto utilizzo dei dispositivi digitali e identificando attuali rischi e minacce provenienti dal web, che ovviamente cambiano e si evolvono nel tempo, seguendo le indicazioni del sito Generazioni Connesse del Ministero dell’Istruzione.

Tra i fenomeni da contrastare vi è sicuramente quello del cyberbullismo, una forma crescente di persecuzione attraverso la rete e i dispositivi digitali fatta di aggressioni, molestie, ricatti e ingiurie tra adolescenti che appare anche più subdola rispetto a quella del tradizionale bullismo.

Come ci ricorda il Ministero dell’Istruzione nelle “Linee guida per l’uso positivo delle tecnologie digitali e la prevenzione dei rischi nelle scuole”, la scuola di oggi ha bisogno di dare risposte adeguate ai nuovi bisogni, creando servizi ad alto valore educativo, che permettano agli studenti di sviluppare le competenze informatiche, per muoversi in sicurezza e con padronanza negli ambienti digitali.

Riferimenti a siti utili:

Generazioni Connesse (www.generazioniconnesse.it)

Cuoriconnessi.it

1. Scopo del documento

Questa Politica d'Uso Accettabile e Sicuro della rete (PUA) vuole fornire un punto di riferimento all'interno dell'Istituto Comprensivo Mezzolombardo Paganella nello sviluppo delle competenze digitali, della sicurezza online e di uso costruttivo delle tecnologie; intende inoltre definire le regole per l'utilizzo dei dispositivi a fini didattici. Infine presenta alcune procedure per la prevenzione dei rischi e per una corretta rilevazione e gestione di eventuali casi problematici.

2. Condivisione e comunicazione della PUA

Mai come in questi tempi abbiamo avvertito la necessità, in qualità di scuola, di stabilire contatti umani anche attraverso l'utilizzo delle tecnologie. Le riunioni fatte da remoto, le video lezioni, gli interventi sincroni e asincroni adottati nella didattica digitale a distanza, ci hanno fatto sperimentare un nuovo modo di entrare nella quotidianità degli studenti, cercando di dare sicurezza quando le condizioni incerte sembravano offuscare il concetto stesso di istruzione. Da queste esperienze ne siamo usciti cresciuti e maggiormente sensibili al mondo della comunicazione attraverso i dispositivi personali.

E' quindi importante riconoscere questa svolta epocale nel mondo della scuola e apprestarsi ad un utilizzo consapevole delle tecnologie, attraverso alcuni concetti fondamentali che riassumiamo qui brevemente:

- **legalità**, nella consapevolezza delle regole della cittadinanza digitale,
- **identità digitale**, nella gestione del proprio esistere in rete,
- **sicurezza**, intesa come software e hardware che ci permettono di non perdere i nostri dati salvati, ma anche che li proteggono da possibili attacchi esterni,
- **privacy / riservatezza**, nel rispetto delle informazioni personali che ci vengono affidate e che dobbiamo saper trattare e custodire.

2.1. Sensibilizzazione delle famiglie

L'intento da parte della scuola è quello di promuovere, insieme alle famiglie, la cittadinanza digitale attraverso una maggiore consapevolezza nell'utilizzo degli ambienti digitali di apprendimento, rispettando la dignità umana e contrastando ogni messaggio di odio, violenza e discriminazione. Durante l'acquisizione delle competenze digitali, la scuola e la famiglia devono essere unite nello sviluppo di un pensiero critico da parte dei giovani, per un uso consapevole delle tecnologie digitali.

Con riferimento al documento Autorizzazione per G Suite For Education, le famiglie sono informate sull'uso della G-Suite for Education, di cui è richiesta autorizzazione scritta all'utilizzo.

Risulta importante una collaborazione reciproca tra scuola e famiglia nell'educazione dei ragazzi e delle ragazze, fondata su di una condivisione di valori e di buone prassi.

La scuola ha organizzato alcuni eventi sia per i ragazzi sia per i genitori:

- **Incontro con il prof. Matteo Lancini**, che si è tenuto il 23 ottobre 2020 in diretta streaming. L'intervento è stato incentrato sull'essere educatori autorevoli al tempo della pandemia e ha trattato anche l'utilizzo consapevole delle tecnologie, indispensabili nella didattica a distanza.

  Link all'incontro sul canale youtube della scuola

- **Safer Internet Day**. Nella giornata mondiale della sicurezza in rete, 9 febbraio 2021, la Polizia Postale e delle Comunicazioni, nell'ambito del progetto #cuoriconnessi, ha realizzato un evento multimediale in diretta streaming. In tale occasione è stato presentato un video documentario costruito sulle testimonianze di vittime di prevaricazione online.
- **Serata Informativa con la Polizia Postale**, in data 18 marzo 2021. L'Istituto Mezzolombardo Paganella con la Consulta Genitori ha organizzato un momento informativo con gli esperti della Polizia Postale, dedicato alle famiglie. L'obiettivo è offrire degli strumenti per esercitare le responsabilità genitoriali sui propri minori in relazione all'uso consapevole della rete e alla gestione in sicurezza di internet.
- Nella serata del 23 febbraio 2021, in diretta online, lo **Spazio Giovani Rotaliana APPM**, in collaborazione con la psicologia Dott.ssa Martina

Rinaldi del Centro Percorso di Trento, ha promosso una serata di formazione ed informazione sul tema della sicurezza online “InformaTi per un internet migliore!”,

Sul sito scolastico saranno resi accessibili i materiali dedicati alle famiglie e agli studenti sulla didattica digitale, sulla sicurezza in rete e sul cyberbullismo scaricabili del sito di “Generazioni connesse” e dal sito “Cuoriconnessi”.

2.2. Formazione dei docenti

Parte fondamentale nella gestione delle tecnologie è sicuramente un’adeguata formazione del personale docente. Tra le iniziative che negli anni si sono ripetute ed hanno incentivato il processo ci sono stati due percorsi principali:

- i **Caffè digitali**, tenuti da docenti esperti dell’Istituto e da esperti esterni, con un approccio interamente laboratoriale, che hanno avuto come oggetto sia l’ambiente delle G-Suite sia le applicazioni esterne ad esso;
- le **formazioni sulle G-Suite** for Education, tenute internamente da un gruppo di insegnanti esperti del nostro Istituto, che hanno condiviso modalità di utilizzo delle varie app presenti. Questo tipo di formazione è periodica e attuata sulle reali esigenze dell’utenza di riferimento.

  Il percorso è iniziato nel marzo 2020 ed è in continua implementazione, in modalità *peer to peer* tra docenti, mediante la condivisione di buone pratiche, la costruzione di materiali come presentazioni, tutorial, etc.

- Nell’A.S. 2020/21 è stato tenuto un corso per l’utilizzo degli **IPad** a disposizione della scuola, al quale hanno partecipato i docenti già coinvolti in sperimentazioni attive nell’Istituto sulla didattica digitale.

2.3. Canali di comunicazione

Il canale principale di comunicazione da parte della scuola è il sito internet:

www.icmezzolombardopaganella.it

Il presente documento sarà reso pubblico nel sito della scuola.

3. Ruoli e responsabilità

E' importante il coinvolgimento di tutti gli attori della scuola: dal Dirigente ai docenti, dagli studenti alle famiglie, seguendo il modello di **scuola come comunità**.

3.1. Dirigente scolastico

Il Dirigente scolastico (DS), nell'ambito della PUA, è tenuto a:

- garantire al personale scolastico una formazione adeguata sulle tecnologie;
- garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza digitale;
- garantire la tutela della privacy di tutti i membri della comunità scolastica.

Il Dirigente si riserva di limitare l'accesso e l'uso della rete interna ed esterna Internet utilizzando un sistema Firewall nel caso di comportamenti poco consoni.

3.2. Animatore digitale

L' animatore digitale (ad) è tenuto:

- alla formazione interna alla scuola sull'utilizzo delle tecnologie informatiche, attraverso l'organizzazione di attività formative, caffè digitali e interventi *peer to peer*, come lo sportello per i docenti;
- al coordinamento nell'Istituto nell'applicazione del Piano Provinciale Scuola Digitale (PPSD), condividendo materiali e partecipando alla comunità degli animatori;
- al coinvolgimento della comunità scolastica, con l'organizzazione di attività sui temi del digitale, anche attraverso momenti formativi aperti alle famiglie e ad altri attori del territorio, per la realizzazione di una cittadinanza digitale condivisa;
- allo sviluppo delle competenze digitali negli alunni attraverso percorsi didattici dedicati e finalizzati alla creazione di un curricolo digitale;
- a fornire un punto di riferimento per le problematiche inerenti internet ed il cyberbullismo.

3.3. Docenti

Tutti i docenti sono tenuti a:

- sviluppare le competenze digitali degli alunni e assicurare un corretto utilizzo di internet e delle tecnologie digitali della scuola;
- segnalare prontamente eventuali problematiche emerse nell'utilizzo dei dispositivi digitali al referente (animatore digitale);
- segnalare al consiglio di classe e al Dirigente scolastico episodi di violazione grave delle politiche sull'uso presentate in questo documento;
- prendere visione della Politica d'Uso Accettabile delle tecnologie all'inizio del rapporto di lavoro.

3.4. Studenti e studentesse

Tutti gli studenti e le studentesse sono tenuti a:

- seguire le indicazioni fornite dalla scuola e condivise dai docenti per un uso corretto e responsabile delle tecnologie digitali.
- rispettare la Netiquette, ovvero le regole di buon comportamento in rete, specialmente in caso di didattica digitale a distanza o da remoto (vedere 6.4.2).

3.5. Famiglie

I genitori saranno informati sulla politica d'uso accettabile e responsabile di Internet e delle TIC a scuola tramite pubblicazione del presente documento sul sito web della scuola. All'atto dell'iscrizione o all'inizio dell'anno scolastico sarà fatto firmare al genitore/tutore dello studente un documento che attesta l'esistenza della PUA, che sarà consultabile sul sito della scuola.

Le famiglie degli alunni/e sono pertanto tenute a:

- contribuire alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- incoraggiare l'impiego responsabile e consapevole delle tecnologie da parte dei giovani,
- condividere con la scuola l'attenzione alla prevenzione dei rischi,

- collaborare nell'attuazione delle procedure previste in caso di violazione delle politiche in uso.

4. Riferimenti normativi

Ministero dell'Istruzione "Linee guida per l'uso positivo delle tecnologie digitali e la prevenzione dei rischi nelle scuole".

Legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo".

Piano Provinciale "Scuola Digitale" (PPSD) del 12 Ottobre 2017.

Piano Nazionale Scuola Digitale (PNSD) (rif. Legge 107/2015).

Ministero dell'Istruzione - Linee di indirizzo "Partecipazione dei genitori e corresponsabilità educativa".

Patto di Corresponsabilità Educativa (DPR 24 giugno 1998, n. 249, modificato dal DPR n. 235 del 21 novembre 2007-art. 5-bis).

Statuto delle studentesse e degli studenti: DPR 24 giugno 1998, n. 249, modificato dal DPR n. 235 del 21 novembre 2007.

General Data Protection Regulation (GDPR) Regolamento Europeo 2016/679.

Codice in materia di protezione dei dati personali - D.Lgs 196/03 e ss.mm.ii.

T.U. sulla sicurezza - D.Lgs 81/08 e ss.mm.ii.

5. Integrazione della PUA con i documenti d'Istituto

La PUA integra e viene integrato dai seguenti documenti programmatici ei regolamenti in essere:

- Progetto d'Istituto
- Piano Digitale d'Istituto
- Regolamento sui diritti, i doveri e le mancanze disciplinari degli studenti approvato dal Collegio Docenti dd 29 giugno 2020.

6. Politica d’uso accettabile

6.1. Utilizzo dei PC portatili

6.1.1. Utilizzo da parte degli alunni sotto la supervisione di insegnanti

La scuola dispone di PC portatili e chromebook che l’insegnante dovrà prenotare presso il tecnico informatico, previa richiesta al DS per scopi didattici.

I PC sono custoditi all’interno di un carrello portatile, dove è possibile ricaricarli.

Nel caso di utilizzo in una determinata ora di lezione, **l’insegnante richiedente dovrà necessariamente supervisionare la distribuzione e l’utilizzo degli stessi**.

Nel caso il CdC prenoti l’intero carrello (nei plessi in cui è disponibile) per utilizzarlo con la classe per un certo periodo (es. una settimana), la tutela dei PC sarà a cura della classe assegnataria, sotto la supervisione di ogni insegnante.

6.1.1.1. Regole di utilizzo dei dispositivi portatili

I dispositivi della scuola sono patrimonio comune, vanno pertanto utilizzati in modo responsabile e lasciati nelle stesse condizioni che avevano prima dell'utilizzo.

E’ severamente **vietato alterare le impostazioni dell’apparecchiatura.** E’ inoltre **vietato installare nuovi programmi**. Ogni eventuale modifica ai software dovrà essere concordata con l’insegnante e verificata dal tecnico informatico.

L'utilizzo dell’apparecchiatura da parte degli alunni **è consentita solo in presenza del personale scolastico** (insegnanti, assistenti educatori) che è pertanto responsabile della sorveglianza sul corretto uso del dispositivo, nonché della navigazione in internet.

L'attrezzatura non deve mai essere lasciata incustodita. Al termine dell'utilizzo ricordarsi di fare il logout dal proprio account istituzionale e di spegnere il dispositivo.

In caso di malfunzionamento o guasto all'apparecchiatura bisogna darne tempestiva segnalazione all'insegnante che contatterà il tecnico informatico.

6.1.2. In comodato d'uso agli alunni

La scuola mette a disposizione degli alunni richiedenti e aventi i requisiti richiesti, PC portatili o chromebook per permettere l'accesso di tutti gli studenti alle attività didattiche a distanza, in piena conformità con le direttive sull'inclusione scolastica e con il principio imprescindibile del diritto allo studio espresso dagli artt. 33 e 34 della Costituzione e dalla rimozione degli ostacoli di ordine economico e sociale, così come garantito dall'art. 3 della Costituzione.

Gli alunni e le alunne assegnatari del bene in comodato d'uso ne divengono anche **responsabili per la custodia ed il corretto utilizzo**, come pure i genitori dei richiedenti in qualità di tutori. Si ricorda in tal senso che la supervisione dell'adulto, che a scuola è garantita con la presenza degli insegnanti, a casa dovrà essere garantita dalla famiglia.

E' severamente vietato alterare le impostazioni dell'apparecchiatura. E' inoltre **vietato installare nuovi programmi.** Ogni eventuale modifica ai software dovrà essere concordata con gli insegnati e preventivamente verificata dal tecnico informatico.

In caso di malfunzionamento, guasto, rottura o perdita dell'apparecchiatura, bisogna darne tempestiva segnalazione alla scuola.

Durante la partecipazione da remoto alle lezioni o alle attività didattiche, seguire la "Netiquette" presentata al punto 6.4.2.

6.1.3. Utilizzo da parte degli insegnanti

L'utilizzo dei PC portatili è possibile da parte di insegnanti e assistenti educatori per scopi didattici. Si possono utilizzare ad esempio per effettuare le lezioni, in particolare i PC portatili presenti nelle aule e collegati alle LIM o ai display multimediali.

Gli stessi possono essere utilizzati anche per i collegamenti durante la didattica a distanza o per le udienze, secondo disponibilità da verificare con il tecnico di laboratorio.

In ogni caso l'insegnante dovrà fare login con le proprie credenziali di accesso (vedere punto 7.2) al dominio scolastico.

E' severamente vietato alterare le impostazioni dei computer. E' inoltre vietato installare nuovi programmi. Ogni eventuale modifica ai software dovrà essere concordata e verificata dal tecnico informatico.

L'insegnante è custode del bene durante l'utilizzo e dovrà tempestivamente segnalare al tecnico informatico ogni danno, malfunzionamento o guasto all'apparecchiatura.

6.2. Utilizzo dei tablet

6.2.1. Utilizzo da parte degli alunni sotto la supervisione di insegnanti

La scuola dispone di alcuni tablet Ipad che possono essere richiesti dagli insegnanti per avviare dei progetti didattici nelle classi. Per l'utilizzo di tali dispositivi sono previste periodicamente sessioni di formazione specifica, come quella avviata nel corrente anno scolastico (vedere punto 2.2).

Gli insegnanti interessati dovranno prenotare i dispositivi presso il tecnico informatico, previa richiesta al DS per scopi didattici.

L'insegnante richiedente dovrà necessariamente supervisionare la distribuzione e l'utilizzo degli stessi durante le proprie ore di lezione.

Durante l'utilizzo seguire le stesse regole presentate al punto 6.1.1. (Regole di utilizzo dei dispositivi portatili)

6.2.2. Utilizzo da parte degli insegnanti

Seguire le stesse istruzioni contenute nel paragrafo 6.1.3.

6.3. Utilizzo dei laboratori informatici

Quanto segue si riferisce ad un contesto Covid free. Qualora vi fosse la necessità di continuare ad applicare le restrizioni legate a protocolli specifici di prevenzione, tali norme prevarranno su quanto qui riportato.

Il laboratorio informatico va inteso come un bene comune messo a disposizione della comunità scolastica e del territorio, pertanto si ricorda che il rispetto e la tutela dello stesso sono condizioni indispensabili per poter fruire di questo bene. **Atti di vandalismo o di manomissione delle attrezzature in esso contenute verranno prontamente segnalate** dal tecnico informatico durante i controlli di routine al DS, che provvederà ad avviare gli opportuni accertamenti dei danni arrecati.

Il laboratorio è inoltre un luogo di lavoro e pertanto soggetto alle leggi sulla sicurezza (vedi T.U. D.Lgs 81-08 e sue successive modifiche o integrazioni) sulla prevenzione degli infortuni, sulla gestione delle emergenze e sulla gestione dei rischi.

6.3.1. Utilizzo da parte degli alunni sotto la supervisione di insegnanti

Gli utenti abituali del laboratorio sono principalmente gli alunni e i docenti dei gruppi impegnati in attività didattiche. Gli studenti della scuola potranno accedere al locale solo se accompagnati da un docente o da altro personale scolastico (es. assistente educatore).

Gli alunni dovranno aver cura di rispettare le procedure corrette di accensione, utilizzo e spegnimento dei PC.

Tutti gli studenti sono responsabili del computer a loro assegnato: pertanto, all'inizio della lezione, è opportuno che comunichino al loro insegnante eventuali malfunzionamenti e segnalino eventuali danni arrecati alla postazione.

L'accesso ai computer, per ragioni di sicurezza, avviene attraverso autenticazione mediante credenziali di accesso (username e password, vedere 7.2) comunicate all'inizio dell'anno scolastico. La password dovrà quindi essere cambiata al primo accesso.

La navigazione su internet degli studenti è intesa come progettata e guidata dai docenti. Gli insegnanti o gli educatori sorveglieranno l'attività degli alunni, che dovrà essere mirata ai soli fini didattici.

Prima di iniziare la navigazione si raccomanda di accedere al proprio account istituzionale (cognome.nome@icmezzolombardopaganella.it) mediante il link alla Gmail presente sul banner di Google.

Al primo accesso, verrà richiesto di cambiare la propria password. Si raccomanda di segnarsi opportunamente le password (accesso PC e accesso alla Gmail istituzionale) e di non condividere l'informazione con nessun altro utente. **È vietato fornire le proprie credenziali d'accesso ad altri.**

E' vietato portare e consumare cibi e bevande nel laboratorio.

Gli alunni sono tenuti a salvare i file personali in cartelle specifiche (in locale, in rete o sul drive istituzionale) come indicato dal personale scolastico. **E' vietato l'utilizzo di chiavette usb o dischi esterni.**

La stampa degli elaborati deve essere autorizzata dagli insegnanti e deve essere limitata alle attività didattiche in corso. Sarà cura dell'insegnante stampare il contenuto dal proprio account attraverso il codice personale per la stampa, comunicato via mail istituzionale.

Al termine dell'utilizzo è cura degli studenti rimettere in ordine la postazione di lavoro: tastiera, mouse, sedia.

6.3.2. Utilizzo da parte degli insegnanti o di altri utenti

Gli utenti del laboratorio quali insegnanti, personale ATA, genitori ed esterni, sono tenuti a mantenere un comportamento consono ad un luogo di lavoro, senza recare disturbo agli altri. E' pertanto necessario mantenere un tono di voce appropriato e limitarsi all'utilizzo di una postazione.

L’attività sul computer e la navigazione su internet degli utenti dovranno essere volte allo svolgimento di attività lavorative quali la progettazione didattica, le attività funzionali all’insegnamento, la compilazione del registro elettronico o l’aggiornamento professionale.

E' vietato portare e consumare cibi e bevande nel laboratorio.

E’ vietato scaricare e installare software (anche a fini didattici) senza previa autorizzazione e verifica del tecnico informatico.

E’ inoltre **vietata l’introduzione di chiavette usb e di hard disk esterni** nelle porte degli elaboratori, se non previa verifica degli stessi presso il tecnico informatico e per ragionevoli motivi (es. backup del lavoro svolto in locale, se non risolvibile attraverso una copia degli stessi nel drive istituzionale).

Come disposizione generale, si raccomanda di ridurre al minimo le stampe, che verranno processate dalla stampante solo previo inserimento del proprio **codice personale per la stampa**, comunicato via mail istituzionale.

Al termine dell’utilizzo **è cura di ogni utente rimettere in ordine la postazione di lavoro: tastiera, mouse, sedia.**

6.4. Utilizzo dei dispositivi personali

6.4.1. Utilizzo a scuola da parte degli alunni sotto la supervisione di insegnanti (BYOD)

L’utilizzo dei dispositivi personali a scuola è consentito solo per motivi didattici. La sperimentazione attuata dalla scuola nei periodi precedenti la stesura di questa PUA, ci permette di definire quanto segue.

Ogni insegnante che intenda attivare la didattica **BYOD** (Bring Your Own Device) dovrà necessariamente informare il DS illustrando le finalità didattiche del progetto. Lo stesso docente provvederà all’invio alle famiglie di un'**informativa (PATTO BYOD)** che alleghiamo al presente documento, da restituire debitamente firmata.

Gli studenti, durante l'utilizzo dei dispositivi in classe, **dovranno osservare le istruzioni impartite dall'insegnante**. E' vietato l'utilizzo del dispositivo per attività non inerenti la didattica ed in particolare **è vietato:**

- **navigare autonomamente** in internet, la navigazione è progettata e guidata dall'insegnante,
- **scattare foto o video** di insegnanti, compagni, strutture scolastiche, se non facente parte del progetto didattico attivato dall'insegnante, previa autorizzazione del DS,
- **postare o condividere foto/video o informazioni** in chat o social quali whatsapp, instagram, tik tok (il cui utilizzo è fortemente sconsigliato anche al di fuori della scuola), facebook, contenitori quali youtube etc.

L'**insegnante**, dal canto suo, sarà **supervisore e tutore** durante le attività in BYOD.

L'insegnante dovrà informarsi dell'effettiva disponibilità dei dispositivi personali all'interno del gruppo classe e provvederà a prenotare i dispositivi della scuola per gli studenti che ne avessero bisogno.

La connessione ad internet avverrà utilizzando la rete wireless della scuola, che prevede un firewall contro le minacce informatiche e una blacklist di siti non navigabili, che viene aggiornata dalla scuola in base ai rischi effettivi o potenziali.

Si raccomanda di **mantenere i dispositivi personali chiusi all'interno dello zaino o dell'armadietto personale** fino all'utilizzo degli stessi sotto la supervisione dell'insegnante. Al termine dell'attività BYOD, i dispositivi andranno rimessi negli zaini / armadietti personali.

Ogni utilizzo improprio sarà disciplinato ed eventualmente sanzionato come da Regolamento sui diritti, i doveri e le mancanze disciplinari degli studenti (vedere punto 2 della sezione 3, Violazione del dovere del rispetto della persona).

6.4.2. Utilizzo da parte degli alunni da remoto (Netiquette)

La registrazione e la diffusione di immagini di minori non autorizzate possono creare gravi problemi come denunce, sanzioni e multe, come pure postare un video fatto da altri.

Durante le video lezioni in Google Meet **è fatto divieto di effettuare riprese, registrazioni audio-video e fotografie di compagni e docenti, a qualsiasi scopo e con qualsiasi mezzo.** È altresì compito delle famiglie sorvegliare i dispositivi impiegati dagli studenti da remoto, al fine di evitare il verificarsi di atti illeciti; si raccomanda inoltre di segnalare qualsiasi eventuale problema ai docenti.

Qualora gli studenti infrangano le suddette regole, gli stessi verranno sanzionati in base a quanto disposto al punto 2 del Regolamento sui diritti, i doveri e le mancanze disciplinari degli studenti, per quanto concerne la violazione del rispetto della privacy.

E' inoltre vivamente consigliato agli studenti il tenere le videocamere accese, per rendere maggiormente partecipativa l'attività didattica da remoto. Nel rispetto della privacy si consiglia di attivare gli sfondi (sfumato/fantasia) disponibili in Google Meet, evitando così di riprendere le stanze della propria abitazione.

E' infine vietato condividere i link alle video lezioni al di fuori della classe.

Si ricorda che la presenza alle video lezioni è da effettuare mediante accesso al proprio account istituzionale: cognome.nome@icmezzolombardopaganella.it

6.4.3. Utilizzo da parte degli insegnanti

Durante le ore di lezione **è consentito l'uso di dispositivi elettronici personali (PC portatili, tablet, smartphone) a scopo didattico ed integrativo di quelli scolastici disponibili.**

Nell'**utilizzo da remoto** dei propri dispositivi (PC, tablet, smatphone) è fatto **divieto di effettuare riprese, registrazioni**

audio-video e fotografie di alunni e docenti, a qualsiasi scopo e con qualsiasi mezzo, nel rispetto della privacy e nella tutela dell'immagine personale.

7. Sicurezza, gestione dell'identità digitale e privacy

Difendersi dalle minacce e dagli attacchi informatici è essenziale per garantire una sicura gestione delle informazioni personali e dei dati che vengono salvati nei dispositivi scolastici e nella rete.

Tra le minacce più diffuse al giorno d'oggi riscontriamo: virus e malwares, worms, trojans, spywares e attacchi o truffe quali phishing, crypto jacking, DDOS, attacchi cyber-fisici, attacchi IoT e furti d'identità.

Per difendersi e minimizzare i rischi informatici si possono attuare le seguenti azioni:

- Installazione di antivirus sui dispositivi e controllo periodico degli stessi,
- Creazione e gestione di profili di accesso ai dispositivi, con username e password in cui controllare autorizzazioni, autenticazioni, privilegi e accessi alle varie cartelle di sistema,
- Utilizzo di sistemi crittografici,
- Installazione di un Firewall di protezione per la rete.

7.1. Sicurezza e accesso ad internet: filtri, antivirus e navigazione

L'accesso a internet è garantito in tutti i plessi scolastici.

Le aule sono dotate di Lavagna Interattiva Multimediale (LIM), sotto forma di videoproiettore o smart tv con annesso un computer portatile. Lo stesso è dotato di software per la LIM e di accesso a internet via LAN o rete wireless.

Per migliorare la sicurezza e nella tutela dei dati personali la scuola ha sottoscritto un contratto nella formula Enterprise per le GSuite Educational di Istituto.

Per gli insegnanti sono disponibili postazioni PC e portatili.

Le impostazioni per l'accesso ai PC sono definite e manutenute dal tecnico informatico per la gestione degli accessi (vedere punto 7.2).

Il tecnico informatico supervisiona il traffico di rete, salvaguardando la sicurezza dagli attacchi esterni per mezzo di software Firewall e controllo della presenza di virus negli elaboratori attraverso antivirus sempre attivi e check periodico con scansione.

Il tecnico informatico provvede anche a installare dei blocchi di navigazione sulla base della compilazione di blacklist, dove vengono inseriti i siti particolarmente rischiosi o non attinenti lo svolgimento di attività didattiche (come nel caso dei social network).

L'aggiornamento periodico di tali blacklist aumenta la sicurezza della navigazione, perché nascono sempre nuovi pericoli in rete.

7.2. Identità digitale: gestione accessi (password, backup)

Le postazioni presenti nell'istituto richiedono password d'accesso personale, gestite, come nel paragrafo precedente, dal tecnico informatico.

Sono previsti quattro profili di accesso con password relative:

- amministratore;
- personale scolastico;
- studenti;
- utenti esterni.

Per questi ultimi è necessario richiedere al tecnico informatico lo username e la password di accesso al PC.

Si ricorda che le password sono soggette a scadenza periodica e quindi vanno rinnovate per poter accedere ai sistemi.

Sia per il personale scolastico che per gli alunni lo username di accesso al dominio scolastico è regolato secondo disposizioni del tecnico informatico, che gestisce la registrazione di ogni nome utente nella rete.

Il tecnico fornisce anche una password temporanea che va sostituita al primo accesso.

Ogni utente dell'istituto ha anche una posta elettronica istituzionale che viene comunicata dal tecnico e che segue il seguente principio di attribuzione della casella di posta GMail:

cognome.nome@icmezzolombardopaganella.it

Il tecnico fornisce anche una password per il primo accesso alla casella, che dovrà essere subito modificata. Si raccomanda di mantenere ben custodite le password di accesso ai computer (dominio scolastico) e alla GMail e di non comunicare a nessuno tali dati, per il rispetto della propria privacy (vedere punto 7.3).

Ogni docente accede al registro elettronico mediante il sito icmezzolombardopaganella.it > Home page > Registro docente, attraverso uno username ed una password fornita dai referenti interni Mastercom.

Nota: L'accesso ai dati riportati nel registro elettronico (voti, ritardi, assenze, note, argomenti, compiti, valutazioni e pagelle) è riservato ai genitori tramite la consegna di username e password di accesso strettamente personale.

A discrezione del Consiglio di Classe, gli studenti possono accedere, dal sito istituzionale, al "quaderno dello studente" dove è possibile consultare compiti, argomenti, voti e materiali didattici. Anche in questo caso username e password vengono fornite dai referenti Mastercom.

7.3. Privacy e protezione dei dati personali

La tutela della privacy è amministrata attraverso la consulenza costante del DPO di Istituto, la Dott.ssa Gioia Cantisani dello Studio Gadler.

Con la consulenza del DPO vengono condivisi con ogni componente della comunità scolastica specifiche mansioni e regole.

Il personale scolastico è pertanto nominato "incaricato del trattamento" da parte dell'Istituto, che, nella persona del DS, è il titolare del trattamento dei dati personali.

Durante l'espletamento delle proprie mansioni (es. compilazione del registro di classe, di materia, partecipazione ai consigli di classe etc.)

ogni insegnante dovrà rispettare il principio di non divulgazione dei dati personali di cui viene a conoscenza.

Tutto il personale autorizzato è stato adeguatamente istruito e formato in riferimento alle modalità di trattamento dei dati personali, ai fini della protezione e della sicurezza degli stessi.

Nel pieno rispetto del GDPR vigente, non è permesso agli insegnanti di pubblicare contenuti riguardanti gli alunni sui propri canali, social o a mezzo internet, su stampa ecc.

Nel caso di progetti didattici specifici, gli insegnanti richiederanno approvazione a pubblicare i dati al DS motivando gli scopi ed il trattamento previsto e poi elaboreranno e distribuiranno apposite liberatoria e informativa agli studenti, da far restituire debitamente compilata e firmata da parte dei genitori/tutori legali.

Per la partecipazione a concorsi/eventi, sia interni che esterni, sarà cura dell'insegnante referente il sincerarsi della necessità di trattamento dati. Se del caso, il docente provvederà alla comunicazione alle famiglie mediante informativa da far restituire all'Ente esterno debitamente compilata e firmata da parte dei genitori/tutori legali.

8. Prevenzione dei rischi, azioni e sistema di rilevazione

8.1. Analisi dei rischi informatici

Il sistema informatico viene costantemente controllato.

- Ogni utente possiede credenziali di accesso personali che non devono essere divulgate;
- La scuola controlla periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni dispositivi digitali.
- È vietato salvare sui dispositivi o scaricare da Internet software non autorizzati.

- Il tecnico informatico si occupa dell'aggiornamento degli antivirus sui dispositivi e alla scansione periodica degli stessi.
- L'utilizzo di chiavette USB o drive esterni è vietato; l'istituto incentiva l'archiviazione dei propri materiali su cloud (Google Drive) e non su supporto esterno, oggettivamente meno sicuro per possibile presenza di virus e difficilmente presidiabile.
- I file di proprietà della scuola sono controllati periodicamente.
- La scuola si riserva di limitare il numero di siti visitabili con filtri blacklist (vedere 7.1) e le operazioni di download relativi.

8.2. Azioni

Il sistema di accesso ad Internet della scuola prevede l'uso di un filtro (attraverso compilazione di blacklist) per evitare l'accesso a siti web che esulino dalla funzione didattica (vedere anche 7.1).

Nel suo funzionamento, il sistema tende a:

- impedire l'accesso a siti non appropriati;
- monitorare e tracciare i collegamenti di ogni dispositivo digitale;
- bloccare e/o consentire l'accesso a risorse in rete attraverso l'uso di parole chiave di ricerca.

Gli utilizzatori devono essere pienamente coscienti degli eventuali rischi ai quali si espongono collegandosi alla rete e che sono identificate ai punti 8.3.1 e 9.1 a cui si rimanda.

8.3. Rilevazione dei casi

La rilevazione è un fattore determinante per la lotta contro i fenomeni e le situazioni a rischio che si possono incontrare online. Il seguente paragrafo fornisce link utili per comprendere le problematiche legate al web.

8.3.1. Situazioni online particolarmente a rischio

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e/o ripetute interazioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile dei social network.

Tra le situazioni a maggior rischio citiamo:

- cyberbullismo,
- hate speech, ovvero incitamento all'odio,
- dipendenza da gioco online,
- sexting e pedopornografia,
- adescamento online.

In particolare si segnaleranno:

- contenuti afferenti la **violazione della privacy** (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- contenuti afferenti all'**aggressività** o che incitino alla **violenza**;
- contenuti afferenti alla **sessualità**;
- **utilizzo eccessivo delle tecnologie** che possano far pensare a problematiche legate a dipendenza.

Per ulteriori informazioni, definizioni e sulle istruzioni operative da adottare per i più comuni pericoli online, si rimanda al VADEMECUM del progetto Safer Internet Centre - Generazioni Connesse.

9. Gestione dei casi

9.1. Infrazioni da parte degli alunni

Sono vietati comportamenti non consoni e/o non legali come:

- scaricare file video-musicali protetti da copyright;
- visitare siti non necessari ad una normale attività didattica;
- alterare i parametri di protezione dei computer in uso;
- utilizzare la rete per interessi privati e personali che esulino dalla didattica;
- non rispettare le leggi sui diritti d'autore;
- navigare sui siti non accettati dalla protezione interna alla scuola.

Nel caso di infrazioni di minore entità, come utilizzo improprio di chat, linguaggio scorretto su bacheche virtuali, comportamento errato nella stesura di documenti digitali condivisi, utilizzo improprio di internet per ricerche non correlate alla didattica, il docente in servizio provvederà a mettere in atto misure di richiamo adeguate a far riflettere sui comportamenti assunti.

Nel caso di infrazioni di maggiore entità, come ad esempio nel caso di danni dovuti alla cattiva cura dei dispositivi scolastici, il docente è tenuto ad informare via mail il Dirigente Scolastico, il coordinatore di classe e l'intero consiglio di classe attraverso comunicazione scritta dell'accaduto. Ovviamente va coinvolta anche la famiglia.

Gli organi coinvolti valuteranno di volta in volta come procedere, anche in applicazione del Regolamento sui diritti, i doveri e le mancanze disciplinari degli studenti approvato dal Collegio Docenti dd 29 giugno 2020.

Per i reati più gravi gli operatori scolastici hanno l'obbligo di **effettuare la denuncia all'autorità** (es. organi di polizia territorialmente competenti).

Utili indicazioni operative si possono trovare anche nel sito del progetto Safer Internet Centre - Generazioni Connesse del Ministero dell'Istruzione e/o contattando telefonicamente l'HELPLINE al numero gratuito 19696 o la chat di Telefono Azzurro.

Per ulteriori informazioni sulle problematiche connesse all'utilizzo delle tecnologie digitali da parte dei giovani, sulle istruzioni operative da seguire e sulle autorità competenti in materia nel territorio si rimanda al VADEMECUM del progetto Safer Internet Centre - Generazioni Connesse.

10. Allegati

Patto BYOD