2022

PUA

POLITICA D'USO ACCETTABILE E SICURO DELLA RETE

Sommario

Premessa e finalità

Due punti fondamentali su cui si focalizza il nostro Istituto in ambito digitale sono rendere i ragazzi fruitori consapevoli e responsabili della rete e diffondere tra il personale le buone pratiche di collaborazione e di condivisione di materiali facendo quindi crescere l'uso delle tecnologie informatiche sia nella didattica che nell'organizzazione generale della scuola. Tuttavia, se da un lato sono immediatamente visibili i vantaggi di un utilizzo di internet e delle tecnologie informatiche sia dal punto di vista didattico che amministrativo, bisogna ricordare che esso può essere anche una potenziale fonte di rischi se non viene utilizzato in modo consapevole e legittimo. Per questo motivo la scuola ha condiviso un Regolamento di laboratorio, riportato a fine documento e appeso in ogni laboratorio informatico, e si appoggia alla Polizia Postale e a esperti esterni per permettere un'ulteriore formazione relativa a rischi e pericoli.

Il presente documento, revisionato ove e quando necessario, costituisce parte integrante del Regolamento interno di istituto.

1. I vantaggi di internet a scuola

La scuola propone l'utilizzo regolare di strumentazioni informatiche attraverso cui gli studenti sono in grado di muoversi in modo autonomo e consapevole nella rete. Internet è una ricca fonte di informazioni per gli studenti e per il personale dell'istituto, ma serve consapevolezza sia delle sue potenzialità, sia dei suoi pericoli.
È infatti buona prassi utilizzare internet non soltanto per le attività sociali, ma anche per promuovere l'eccellenza e l'innovazione attraverso la condivisione di risorse, progetti e scambi culturali stando però attenti ai rischi in cui si può incorrere online. Per questo motivo la scuola limita l'accesso a internet mediante un filtro per la navigazione implementato sul firewall di rete, le attività svolte vengono monitorate e tracciate nel rispetto delle vigenti normative sulla privacy e gli insegnanti si attengono al presente regolamento nel condurre attività online con e per gli studenti.

2. Strategie della scuola per garantire la sicurezza delle TIC

Le strategie attuate dall'istituto per garantire la sicurezza delle TIC sono:

- la limitazione dell'uso della rete interna ed esterna attraverso l'utilizzo dei comuni canali di protezione presenti nel sistema operativo in uso e di Proxy/Firewall per gli studenti e Trentino Network per gli uffici amministrativi;
- la sensibilizzazione e la diffusione di buone pratiche che portano a evitare di:
    - scaricare e/o diffondere materiale protetto da diritto di utilizzo (copyright) rispettando così il diritto d'autore;
    - utilizzare la rete per interessi privati e/o non consoni all'attività svolta e al ruolo ricoperto;
    - modificare i parametri di protezione dei computer in uso e/o installare software senza previo consenso da parte dei tecnici.

Per incrementare il livello di sicurezza si ricorda inoltre che:

- il sistema informatico viene mantenuto e controllato periodicamente e i suoi sistemi di sicurezza vengono aggiornati;
- a fine anno scolastico viene effettuata una pulizia del profilo di ogni singolo utente;
- è necessario il consenso e l'autorizzazione dei tecnici per salvare sul server e/o scaricare da internet software di qualsiasi natura, o utilizzare software precedentemente caricati su supporti esterni di memoria,
- l'utilizzo di supporti esterni personali (precedentemente controllati con l'antivirus) è consentito

se autorizzato dal docente;
- per evitare problemi di privacy al termine di ogni sessione di lavoro la connessione deve essere chiusa effettuando il logout (è in uso il browser Brave che alla chiusura della finestra applicativa disconnette automaticamente tutti gli eventuali account attivi);
- sono limitati i siti visitabili e le operazioni di download;
- è vietato diffondere intenzionalmente virus, worms o altri codici che possano danneggiare, modificare o trasferire dati.

3. Accertamento dei rischi e valutazione dei contenuti di internet

L'utilizzo di Internet durante l'orario scolastico è consentito solo per usi didattici e previo consenso del docente.
Per tutelare gli studenti, la scuola ha previsto un filtro, per evitare l'accesso a siti web con contenuto inopportuno all'attività didattica e all'età dell'utenza, il monitoraggio e la tracciatura di quanto svolto su ogni macchina.
Essendo consapevoli che queste strategie potrebbero non essere sufficienti, vi è la possibilità di richiedere da parte degli insegnanti un eventuale blocco di internet per gli studenti che non lo utilizzino in modo idoneo. Per sviluppare negli studenti una consapevolezza nell'uso responsabile della rete, all'interno dell'istituto vengono inoltre svolti degli incontri con organi competenti ed esperti esterni.

3.1 Sicurezza e Uso delle TIC

Utilizzo dei servizi internet

- L'insegnante promuove un utilizzo consapevole di internet presso gli studenti ed è responsabile di quanto avviene durante le proprie ore di lezione.
- Durante le ore di lezione e le attività extracurricolari pomeridiane è necessario utilizzare l'account di istituto.
- I laboratori e tutti i dispositivi disponibili in istituto possono essere utilizzati esclusivamente per scopi inerenti al proprio ruolo.
- Gli studenti possono accedere a laboratori e postazioni solo sotto diretta supervisione di un docente.

Sicurezza della rete interna (LAN)

L'istituto dispone di un dominio su rete locale solo a livello amministrativo. È prevista una fornitura DHCP per l'assegnazione automatica di un indirizzo di rete e, per ragioni particolari, è possibile richiedere l'assegnazione di un indirizzo IP locale statico.
La rete interna è protetta da un Proxy/Firewall per quanto riguarda le connessioni con l'esterno e ogni postazione è protetta con sistemi antivirus regolarmente aggiornati.

Sicurezza della rete senza fili (Wireless – WiFi)

La scuola offre una copertura WiFi in tutto l'istituto. A tale rete, regolata da un server specifico con filtraggio degli accessi, è possibile accedere solo dopo aver fornito al tecnico il MAC ADDRESS del proprio dispositivo da connettere.

4. Norme e linee guida

Tutti gli utenti devono sottostare alla vigente legislazione ma la scuola, per tutelare ulteriormente l'accesso a internet, applica un filtro, controllato dai tecnici informatici, per evitare la consultazione di informazioni o siti web inopportuni e per monitorare i siti visitati da tutti gli utenti connessi alla rete.
Dopo un certo numero di violazioni il dirigente scolastico si riserva il diritto di bloccare o limitare l'accesso a internet agli utenti interessati.

4.1 Gestione del sito web della scuola

La gestione del sito web dell'istituto, la rispondenza alle normative e le tecniche di realizzazione e progettazione sono a cura dell'Animatore Digitale dell'istituto, nel rispetto della pubblicazione di contenuti pertinenti alle finalità educative istituzionali rispettando la normativa vigente in relazione alla privacy degli utenti interessati.

4.2 Mailing list moderate, gruppi di discussione e chat room

La scuola ha la facoltà di inviare documenti utilizzando delle liste di indirizzi di particolari gruppi di utenti.
Nel caso in cui, durante le attività didattiche, vengano utilizzate chat o altri mezzi di collaborazione come quelli presenti nella Goggle Workspace, l'insegnante viene considerato quale moderatore di tali comunicazioni. Agli studenti d'altra parte è permesso l'accesso alla chat solo per scopi inerenti alla didattica, mentre non è consentito l'accesso alle chat non moderate.

4.3 Linee guida di utilizzo delle TIC all'interno dell'istituto

Per tutti gli utenti (studenti, personale docente, personale ATA, famiglie e ospiti)

Valgono i seguenti punti:

- non è possibile utilizzare giochi né in locale né in rete, se non per scopo strettamente didattico. • È necessario salvare sempre i propri file in cartelle personali e/o di classe o dei docenti, su dispositivi di memorizzazione esterni o su cloud e non su hard disk locale per questioni di spazio.
- Si raccomanda di salvaguardare il più possibile e non diffondere i propri dati personali, soprattutto quelli sensibili (indirizzo, recapiti telefonici, data di nascita, orientamento religioso, politico, sessuale…) e di evitare incontri con sconosciuti trovati in rete.
- È necessaria l'autorizzazione sia per scaricare e/o caricare qualsiasi tipo di materiale dalla rete, sia per iscriversi a qualsiasi concorso con l'indirizzo dell'istituto.
- È necessario riferire al proprio insegnante/al dirigente scolastico se si ricevono via email o tramite messaggistica immagini inappropriate; non bisogna rispondere a tali comunicazioni o provocazioni e/o inviare messaggi offensivi, illeciti o inappropriati.
- Non si è autorizzati ad inviare email personali né ad utilizzare internet per scopi non inerenti alla mansione svolta.
- L'uso dei dispositivi e l'accesso a internet sono tracciabili per motivi di sicurezza e nel rispetto delle normative della privacy.

Inoltre, per ciascuna componente:

Studenti

- L'email istituzionale del gruppo classe o del gruppo studenti è riservata esclusivamente a comunicazioni di tipo didattico/organizzativo.
- La violazione consapevole della PUA della scuola comporta la temporanea sospensione dell'accesso ad internet per un periodo commisurato alla gravità del fatto. La violazione o il dolo accertati comportano un provvedimento disciplinare stabilito dal consiglio di classe; rimangono comunque applicabili ulteriori sanzioni disciplinari, azioni civili per danni, nonché l'eventuale denuncia del reato all'autorità giudiziaria.

Docenti

- È necessario discutere con gli alunni della PUA della scuola e degli eventuali problemi che possono verificarsi nell'applicazione delle regole riguardanti gli strumenti messi a disposizione dalla scuola, fornendo chiare indicazioni su come utilizzare internet e tutte le applicazioni della GSuite, e ricordando che le navigazioni saranno monitorate.
- Si raccomanda di avvisare gli alunni che la violazione consapevole della PUA della scuola comporta la temporanea sospensione dell'accesso ad internet per un periodo commisurato alla gravità del fatto.
- Nel caso di infrazione consapevole da parte dei docenti sarà compito del dirigente scolastico intervenire per via amministrativa secondo le norme vigenti.

Personale ATA

- È vietato far entrare gli alunni nei laboratori a meno che non vi sia l'insegnante o un tecnico informatico.
- Nel caso di infrazione consapevole da parte del personale ATA sarà compito del dirigente scolastico intervenire per via amministrativa secondo le norme vigenti.

Famiglie

- Si raccomanda di promuovere presso i propri figli l'attenta lettura e l'osservanza della PUA della scuola.
- Per le comunicazioni e riunioni online con i docenti è necessario utilizzare esclusivamente l'account di posta istituzionale.

Ospiti

- È vietato installare applicativi sui computer di proprietà dell'istituto.
- L'accesso alla rete WiFi è permesso solo con l'autorizzazione del dirigente scolastico, a cui dovrà preventivamente essere inoltrata tale richiesta specificando data e periodo dell'accesso.

4.4 Altre forme tecnologiche di comunicazione

Gli studenti possono utilizzare dispositivi personali (pc, smartphone, smartwatch, tablet e simili) durante le lezioni o durante l'orario scolastico esclusivamente per attività didattiche, previa autorizzazione e sotto la stretta supervisione di un docente. Ai docenti e al personale che entra in diretto contatto con gli allievi, è altresì vietato l'uso di dispositivi personali (pc, smartphone, smartwatch, tablet e simili) durante lo svolgimento delle lezioni, se non per scopi didattici.

5. Comportamento in rete e uso consapevole delle tecnologie

Come per la vita quotidiana anche su internet esistono delle regole implicite di bon ton che prendono il nome di netiquette. Questo documento contiene le linee guida di buon comportamento e di sicurezza che vanno rispettate mentre si è connessi alla rete. A questo proposito, si segnala il manifesto della comunicazione non ostile, particolarmente utile per la comunicazione online.

5.1 Principi Generali

1. Internet favorisce la libertà di espressione e vanno sempre segnalati i comportamenti e i contenuti che vengono reputati inadatti o offensivi in modo da mantenere la rete un luogo sicuro.
2. 2. Quando si naviga sui social network è necessario tener conto dei diritti e dei doveri degli utenti.
3. È necessario prestare attenzione a quello che viene condiviso online e a alle persone con cui vengono condivise tali informazioni cercando sempre di proteggere la propria e l'altrui identità digitale.

5.2 Comportamenti nelle relazioni tra persone di pari livello – (Rapporto 1 a 1)

1. È necessario prestare attenzione ai documenti, al materiale audiovisivo e alle informazioni che vengono condivisi con le persone conosciute online, poiché sui social network le interazioni che si instaurano non sono veicolate o controllate da intermediari.
2. Nel caso in cui venisse riscontrato un comportamento riconducibile ad un illecito è consigliato segnalare tempestivamente tale fatto attraverso i canali opportuni abbandonando eventualmente la conversazione o cambiando profilo.
3. È bene evitare di aprire file sospetti e aggiornare costantemente l'antivirus.
4. È vietato scaricare o condividere materiale illegalmente.
5. È vietato divulgare informazioni personali di altri utenti o spam.

5.3 Creazione e diffusione di contenuti generati dagli utenti – (Rapporto 1 a N)

1. È importante cercare di salvaguardare la propria e l'altrui privacy, utilizzando i corretti livelli di sicurezza e chiedendo il permesso ai diretti interessati o ai loro genitori/tutori nel caso siano minorenni, prima di pubblicare materiale contenente informazioni o materiale audiovisivo su terze persone.
2. È importante ricordare che tutto quello che viene condiviso in rete è persistente e spesso molto difficile da eliminare.
3. Quando si fa parte di una community, è necessario essere coerenti con il contesto ed evitare di pubblicare materiale inopportuno o che violi il regolamento interno.
4. Nel caso in cui venga utilizzato un nuovo servizio è necessario informarsi su quali siano gli strumenti per segnalare comportamenti o materiali inadatti o ritenuti offensivi.

5.4 Gestione delle relazioni sociali – Communities – (Rapporto N a N)

1. Considerando che le relazioni che si sviluppano su un social network sono simili a quelle reali è importante avere interazioni solamente con persone che si ritengono affidabili, con cui si è a proprio agio e di cui si conosca la reale identità.
2. Nel caso in cui non si conosca la reale identità di un utente incontrato in rete è importante non condividere dati sensibili e contenuti privati, soprattutto se riguardano terze persone. 3. Nel caso in cui, per un errore di attribuzione dei livelli di privacy, si trovassero informazioni personali e private di altri utenti è opportuno segnalarlo al diretto interessato evitando di leggere tali documenti.
3. La reputazione digitale è persistente ed equivale a quella reale: pertanto non bisogna diffamare le persone online, soprattutto se le stesse non sono presenti sul social network e non possono quindi accorgersi del danno subito e difendersi.

5.5 Cyberbullismo

Con il termine “cyberbullismo” si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali realizzati, per via telematica, a danno di minori, nonché la diffusione di contenuti on line riguardanti uno o più componenti della famiglia di un minore con lo scopo di isolarlo, attaccarlo o metterlo in ridicolo.
La legge n. 71/2017 consente ai minori di chiedere l’oscuramento, la rimozione o il blocco di contenuti, a loro riferiti e diffusi per via telematica, che ritengono essere atti di cyberbullismo (ad esempio, foto e video imbarazzanti o offensive, oppure pagine web o post sui social network in cui si è vittime di minacce, offese o insulti, ecc.). Il gestore del sito entro 24 ore deve dare comunicazione di aver preso in carico la richiesta e deve rimuovere contenuti illeciti e dati personali della vittima entro 48 ore. Qualora ciò non avvenga, la vittima può rivolgersi al Garante per la protezione dei dati personali, il quale dovrà provvedere entro quarantotto ore alla rimozione.
Inoltre, la normativa prevede anche una procedura di ammonimento, attuabile nel caso di illeciti su internet (commessi da minorenni di più di 14 anni nei confronti di altri minori) per i quali non sia ancora stata presentata querela o denuncia. In questo caso, il questore è tenuto a convocare il colpevole insieme a un genitore e a registrare l’ammonimento.
Nel caso si venga a conoscenza di atti di cyberbullismo nel contesto scolastico, si è tenuti a informare tempestivamente il coordinatore di classe e/o il referente di istituto preposto.

6. Responsabilità sulla Politica d’Uso Accettabile (PUA) della scuola

6.1 Responsabilità degli studenti sulla PUA della scuola

Gli studenti sono tenuti a sottoscrivere il documento, a impegnarsi nel rispetto delle regole in esso contenute, assumendosi le responsabilità di propria competenza. Gli studenti sono supportati dai docenti nella lettura e comprensione della PUA.
Il Regolamento di laboratorio, riportato alla fine del presente documento, è affisso in ogni aula informatica.

6.2 Responsabilità del personale scolastico sulla PUA

Il personale scolastico si aggiorna sull'utilizzo consapevole della rete e sulle problematiche relative ai diritti d'autore ed è tenuto a sottoscrivere il presente documento, assumendosi le responsabilità di propria competenza.
Gli insegnanti hanno la responsabilità di informare gli studenti dei contenuti della PUA d'istituto considerando la loro età e discutendo opportunità e rischi connessi all'uso delle TIC e di dare le istruzioni per un utilizzo sicuro e responsabile della rete per cui vengono inoltre svolti periodici incontri di formazioni con organi competenti o esperti del settore.

6.3 Responsabilità dei genitori/tutori sulla PUA della scuola

I genitori e i tutori vengono informati della PUA d'istituto e, nel caso in cui gli studenti fossero minorenni, vengono chieste loro le autorizzazioni all'uso di internet e alla pubblicazione dei loro lavori e di eventuali immagini sul sito web della scuola.
I genitori e i tutori sono tenuti a sottoscrivere il presente documento, assumendosi le responsabilità di propria competenza.

7. Disposizioni di legge e sanzioni

7.1 Reati e violazioni della legge

Oltre alla netiquette, è importante ricordare che alcuni comportamenti, ritenuti erroneamente innocui, possono portare gli utenti a commettere veri e propri reati penalmente perseguibili. A tal proposito si citano alcuni esempi tratti dalla Gazzetta Ufficiale delle Repubblica Italiana (legge 547/93 e successive modifiche):

- Accesso abusivo a un sistema informatico o telematico
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche
- Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche
- Danneggiamento di sistemi informatici e telematici
- Frode informatica

7.2 Reati non informatici

Oltre ai reati informatici è bene ricordare che esistono altri reati che possono essere perpetrati in rete in cui la tecnologia informatica non sia un fattore determinante per il compimento dell'atto. A titolo di esempio, nel sito web dello Studio Cataldi, si può trovare:

- "Il reato di ingiuria di cui all'art. 594 c.p. è commesso da chiunque offenda "l'onore o il decoro di una persona presente". La pena prevista è la reclusione fino a sei mesi o la multa fino a 516 euro, fatte salve le aggravanti di cui al terzo e al quarto comma se l'offesa consiste nell'attribuzione di un fatto determinato o se è stata commessa in presenza di più persone."
- "La diffamazione è un reato previsto e punito dall'art. 595 c.p. e che consiste nell'offesa all'altrui reputazione fatta comunicando con più persone. Ai fini della configurabilità del reato di diffamazione è necessario che la persona offesa non sia presente o, almeno, che non sia stata in grado di percepire l'offesa."
- "Nel nostro ordinamento il diritto d'autore è regolato dal Codice Civile, libro quinto, titolo IX, capo I,

agli articoli 2575-2583 c.c. e dalla Legge n. 633, del 22 aprile 1941, "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio". Tale legge, a seguito degli innumerevoli sviluppi sia commerciali che tecnologici, ha subito diverse modifiche e aggiornamenti. Su tale materia è, anche, intervenuta l'Unione Europea con trattati e convenzioni internazionali. L'articolo 1, della L. 633 del 1941, definisce quali siano le opere sottoposte a tale tutela: "Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione". Ricadono nell'ambito di tale tutela anche i programmi per computer (software) e le banche dati. Prima di passare alla disamina degli strumenti di tutela che il Legislatore ha previsto in sede civile e in sede penale è d'uopo, in primis, soffermarsi sul concetto di diritto d'autore."

- "La minaccia è un delitto contro la libertà individuale della persona, punito dal codice penale con una multa (fino a 1.032 euro) e, nei casi più gravi (previsti dal secondo comma dell'art. 612 c.p.), con la reclusione fino a un anno."
- "Il reato di molestie previsto dall'art. 660 del codice penale punisce "chiunque in luogo pubblico o aperto al pubblico, ovvero col mezzo del telefono, per petulanza o per altro biasimevole motivo, reca a taluno molestia o disturbo" con l'arresto fino a sei mesi o con l'ammenda fino a 516 euro."

7.3 Sanzioni

Facendo riferimento al Regolamento dei diritti e dei doveri degli studenti reperibile sul sito dell'istituto, vi è la possibilità, su valutazione dei tecnici informatici, del consiglio di classe e del dirigente scolastico, di impedire l'accesso alla rete per un periodo di tempo conforme alla gravità dell'atto compiuto e/o di informare l'autorità giudiziaria.
Nel caso in cui l'infrazione venga commessa dal personale scolastico vi potrà essere l'intervento per via amministrativa del dirigente scolastico.
Nel caso in cui l'infrazione venga commessa da un ospite, il dirigente scolastico informerà l'autorità giudiziaria, se del caso.

7.4 Alternative al Copyright

Per evitare di incorrere in sanzioni dovute a violazioni del Copyright è possibile utilizzare software liberi e gratuiti che svolgono le stesse funzioni dei pacchetti protetti da Copyright e/o cercare materiali coperti dal licenze Creative Commons (http://www.creativecommons.it/).

8. Controlli

Il datore di lavoro può riservarsi di controllare il corretto utilizzo degli strumenti di lavoro, pertanto il dirigente scolastico, o un suo delegato, può controllare i singoli computer o il server per accertare eventuali violazioni del presente regolamento.

Regolamento Laboratori di Informatica

In riferimento all'Art. 30 del Regolamento Interno di istituto, seguono alcune precisazioni in merito al regolamento per l'utilizzo delle aule informatiche nei plessi scolastici.

Postazioni

1. Ogni utente è direttamente responsabile della postazione che utilizza.

Utilizzo dispositivo

2. Non sono ammesse attività di tipo ricreativo, pertanto è vietato installare, copiare e utilizzare giochi.
3. Gli studenti e il personale della scuola possono utilizzare le attrezzature informatiche presenti purché la finalità sia di tipo professionale. È consentito l'utilizzo di periferiche di massa personali per l'archiviazione e la memorizzazione dei propri documenti/elaborati solo dopo un controllo antivirus.
4. È vietato modificare le configurazioni di sistema delle attrezzature informatiche e di rete tese ad influenzare negativamente la regolare operatività.
5. È vietato inserire password per bloccare o disabilitare qualsiasi funzione o documento. Tutti i documenti dovranno essere in chiaro, non protetti, non criptati anche per garantire l'esecuzione di copie di archiviazione (backup).

Segnalazione problemi

6. In caso di sospetto uso illecito della strumentazione il dirigente scolastico potrà prendere visione e conoscenza dei flussi informativi legati alle sessioni di interesse.
7. È fatto obbligo di segnalare tempestivamente eventuali danni, carenze, obiezioni, situazioni di disordine, sporcizia, anomalie varie ecc., nonché di uscire dal programma utilizzato prima di spegnere l'elaboratore, onde evitare danni irreparabili.

Navigazione online

8. L'utilizzo delle attrezzature informatiche presenti nella rete di istituto è unicamente legato a scopi didattici. Nella rete sono attivi degli strumenti che tengono traccia di tutte le attività svolte all'interno (rete locale) o all'esterno (rete internet). Il dirigente scolastico, quale responsabile delle attività svolte in rete, dispone di strumenti di analisi del traffico generato dagli utilizzatori in rete locale e internet.
9. L'accesso alla rete e ai suoi servizi cesserà d'ufficio alla scadenza del rapporto/collaborazione dell'utente con l'istituto, secondo le informazioni comunicate dalla segreteria scolastica.
10. È vietato consultare servizi internet per scopi non legati alla didattica; in particolare utilizzare materiale in violazione dei diritti d'autore e di copyright e consultare:
    - materiale offensivo incluse espressioni diffamatorie, di fanatismo, razzismo, odio, ecc.; • materiale che promuove o fornisce informazioni su attività illegali;
    - siti web contenenti materiale pornografico;siti web contenenti proposte di acquisto di beni ad uso privato;
    - materiale contenente componenti potenzialmente dannosi;
    - materiale legato al gioco d'azzardo in genere.
11. La messa in opera di chat, blog, forum e forme simili di espressione del pensiero in internet, esterne alla piattaforma dell'istituto, ricadono sotto la piena responsabilità di chi le attiva.
12. L'attivazione del servizio wi-fi è autorizzata (al solo personale docente) dal dirigente scolastico previa compilazione del modulo di attivazione. Il servizio consente, con attrezzature informatiche personali, di accedere alla rete internet, controllata e monitorata da appositi strumenti di analisi.
13. Ogni collegamento dovrà essere chiuso al termine di ogni sessione di lavoro.
14. I docenti sono responsabili di quanto avviene durante le proprie ore di laboratorio.

15. Ogni utente è tenuto a rispettare le regole di decenza e morale per evitare atti e comportamenti che possano recare offesa a cose, persone o istituzioni presenti o meno sulla rete.
16. Gli studenti sono tenuti a riferire all'insegnante eventuali ricezioni di immagini e/o materiali inopportuni.

Uso dei laboratori

17. L'accesso ai laboratori di informatica è consentito solo alla presenza del personale docente o tecnico in grado di assicurare assistenza funzionale e didattica.
18. Durante i periodi di sospensione dell'attività didattica non è consentito l'utilizzo dei laboratori, salvo autorizzazione specifica rilasciata dal dirigente scolastico.
19. Nei laboratori di informatica è ammesso solo lo stretto necessario; eventuali borse, zaini e cartelle vanno posizionati in modo da lasciare libero il passaggio tra le postazioni; giubbotti e giacche vanno posizionati sugli appositi appendiabiti nella classe di provenienza.
20. È vietato consumare alimenti nel laboratorio, sia per evidenti motivi di igiene sia per evitare danni alle attrezzature informatiche.
21. È obbligatorio spegnere eventuali telefoni cellulari o apparecchiature elettroniche di qualsiasi genere, come richiamato anche dal regolamento sui diritti e doveri degli studenti e dei comportamenti che configurano mancanze disciplinari.
22. I laboratori sono adibiti a luogo di studio; non è pertanto ammesso disturbare gli altri utenti parlando ad alta voce o sostando senza motivi all'interno dello stesso.
23. L'orario programmato dovrà essere rigorosamente rispettato. Eventuali prenotazioni fuori orario dovranno essere concordate dal docente con il personale tecnico almeno un giorno prima. In caso di sostituzione del docente assente è possibile utilizzare l'aula di informatica solo per proseguire o rinforzare un'attività già iniziata o prevista dai programmi per la quale il docente abbia la competenza e l'autonomia necessaria.
24. Nei laboratori di informatica possono accedere solo gli studenti appartenenti alla classe indicata dall'orario stabilito, non è consentita la presenza contemporanea di più classi se non per particolari iniziative preventivamente autorizzate dal dirigente scolastico.
25. Per l'uscita dal laboratorio in caso di emergenza ci si deve attenere alle disposizioni date ed illustrate in ogni locale dell'edificio e portarsi nel luogo di ritrovo indicato, interrompendo immediatamente ogni attività.

Materiale presente e utilizzo software

26. Chi accede ai laboratori è tenuto al più scrupoloso rispetto di tutte le attrezzature presenti. Il sistema operativo, il software applicativo e l'hardware messi a disposizione non possono essere utilizzati per attività personali o a fini di lucro. Il software non può essere copiato e distribuito su installazioni esterne all'istituzione scolastica.
27. È vietato l'uso e il possesso di programmi atti a violare la sicurezza dei sistemi locali e remoti.
28. È vietato a chiunque non sia autorizzato installare programmi, modificare installazioni di programmi e di rete, cambiare le configurazioni delle macchine.
29. I laboratori sono dotati di materiale inventariato come hardware, software, manuali e testi da utilizzare per scopi didattici che sono custoditi in appositi armadi.

Personale tecnico

30. L'accesso alla rete e l'efficienza dei relativi servizi sono assicurati dallo staff tecnico che può proporre modifiche e/o integrazioni a questo regolamento ove richiesto da motivazioni di carattere tecnico, d'opportunità, o per l'emergere di situazioni ed ambiti non contemplati che necessitano di essere disciplinati.
31. L'installazione dei programmi o l'operatività e affidabilità delle attrezzature è di competenza dei tecnici informatici.

L'aula informatica SSPG Cognola è organizzata nel seguente modo:

- È dotata di una postazione docente con microfono e gestione della LIM/proiettore e di 24 postazioni studente,
- l'accesso è gestito tramite prenotazione online (a cura del docente, tranne che per le ore di Informatica in orario scolastico già prenotate-riservate in calendario),
- la prenotazione può essere effettuata accedendo al relativo Calendario (PRENOTAZIONE LABORATORIO INFORMATICA) di Google Calendar,
- l'aula Informatica viene già prenotata per l'intero anno scolastico per l'ora didattica di Informatica (compresenza docenti di Matematica e Tecnologia). Queste ore hanno accesso prioritario rispetto ad altre eventuali prenotazioni in quanto incluse in orario didattico e formalizzate nel Progetto d'Istituto (all'interno di queste ore i docenti di Matematica delle classi terze potranno anche svolgere esercitazioni per le prove INVALSI),
- fare attenzione alle nuove prenotazioni in quanto il Calendario è aperto a tutti i docenti SSPG sia in lettura ma anche in modifica. In caso di errori, difficoltà e/o cancellazione di eventi precedentemente inseriti per Informatica o da altri colleghi, inviate una email di richiesta supporto (in questi casi, se è stato cancellato uno o più eventi relativi ad un'ora istituzionale di Informatica, la classe prevista da orario scolastico avrà precedenza di accesso rispetto ad altre errate prenotazioni),
- per l'accesso alla rete internet (per utilizzare le applicazioni Google Workspace, componente principale del programma annuale di Informatica) per i docenti e studenti, bisogna inserire delle credenziali personali dell'account istituzionale assegnato,
- per motivi di sicurezza e privacy è fortemente sconsigliato l'uso di chiavette usb, ma si invita fortemente a lavorare con file nel Google Drive del proprio account istituzionale,
- Per consentire, negli spazi orari diversi da Informatica, una maggiore e più ampia fruizione dell'aula Informatica ai docenti interessati ogni docente può prenotare spazi orari nella settimana corrente e/o al massimo nella settimana successiva a quella corrente. Eventuali prenotazioni non conformi a questa indicazione potranno essere cancellate dal calendario. Vi invitiamo gentilmente ad avvisare il collega che ha effettuato la prenotazione (cliccando sull'evento del calendario, in basso a sinistra è visibile il campo "Creato da:" con il nominativo del relativo docente), e solo successivamente cancellare la prenotazione o modificare i dati della prenotazione con la propria classe/titolo dell'evento. Nota: alcuni eventi come esercitazioni prove INVALSI, attività per educazione alla cittadinanza digitale (cyberbullismo, ...), ecc. potranno avere deroga a tale procedura, e quindi ad esempio il docente referente potrà prenotare l'aula Informatica anche in un periodo che supera le due settimane dalla data corrente.

Regolamento Prenotazione tablet iPad (SSPG)

Sono disponibili anche alcuni dispositivi mobili del tipo tablet Android e ipad Apple.

Gli ipad possono essere prenotati ed utilizzati in classe tramite il seguente calendario: PRENOTAZIONE TABLET IPAD (prendere visione del regolamento per l'utilizzo e prenotazione dei tablet - disponibile nel Drive condivisi, cartella "ELENCHI EMAIL-INFORMATICA e RETE della scuola").