FUTURA LA SCUOLA PER L'ITALIA DI DOMANI

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Istruzione e del Merito

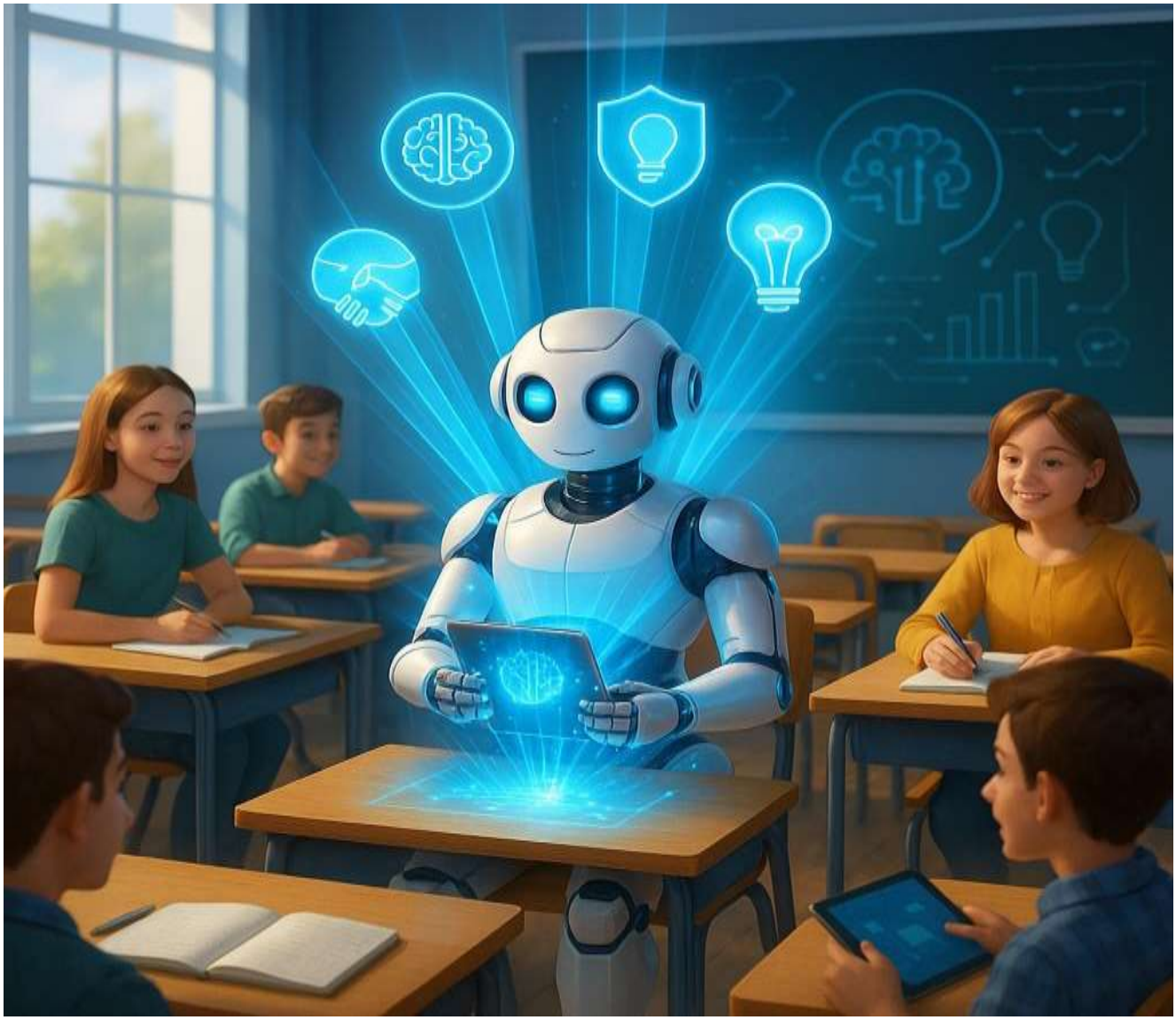
Italiadomani

Istituto Comprensivo Statale "C. Ederle"

C.so Fraccaroli, 58 – 37049 Villa Bartolomea (VR)
Tel. 0442/1833810 – **Sito**: www.icvillabartolomea.edu.it
e-mail: vric84600r@istruzione.it - **PEC**: vric84600r@pec.istruzione.it

PROCEDURE OPERATIVE

PER L'USO DI STRUMENTI INFORMATICI





L'introduzione dell'IA deve rispondere ai principi di trasparenza, etica, sicurezza e inclusività, nell'ambito di un processo educativo che rispetti i diritti e la dignità degli studenti e del personale.



Articolo 1 - Scopo e Obiettivi

1. L'Intelligenza Artificiale è utilizzata nella scuola come strumento di supporto al **processo educativo**, **amministrativo** e **organizzativo**.
2. Gli obiettivi principali sono:
    - Migliorare l'efficacia dell'insegnamento e dell'apprendimento.
    - Facilitare la personalizzazione dei percorsi formativi per ogni studente.
    - Automatizzare attività amministrative, riducendo il carico burocratico.
    - Promuovere competenze digitali avanzate tra studenti e docenti.



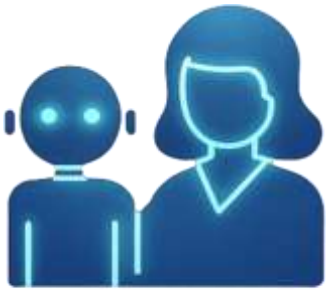
Articolo 2 - Principi Fondamentali

1. **Centralità della Persona**: L'uso dell'IA deve rimanere uno strumento al servizio degli studenti, docente e della comunità scolastica, senza mai sostituire l'intervento umano.
2. **Equità e Inclusività**: Le tecnologie IA non devono creare disparità tra gli studenti. È necessario evitare qualsiasi forma di discriminazione o pregiudizio.
3. **Trasparenza**: Ogni sistema IA utilizzato deve essere comprensibile e spiegabile, con modalità di accesso trasparenti per studenti, docenti e famiglie.
4. **Sicurezza e Privacy**: Tutti i dati personali degli studenti devono essere trattati in conformità con la normativa vigente in materia di privacy (GDPR).
5. **Sostenibilità**: L'utilizzo delle tecnologie IA deve rispettare l'ambiente e favorire una **sostenibilità digitale**.
6. **Minimizzazione e pseudonimizzazione obbligatorie**: non inserire MAI dati reali identificativi nei sistemi di IA. Utilizzare solo pseudonimi o dati non riconducibili a persone reali.
7. **Responsabilità individuale**: ogni operatore è personalmente responsabile dell'uso che fa degli strumenti di IA. L'Istituzione scolastica non si assume responsabilità per eventuali usi impropri.



Articolo 3 - Uso dell'IA nella Didattica

1. **Sistemi di supporto all'insegnamento**: L'IA può essere utilizzata per supportare la personalizzazione dell'apprendimento e per offrire risorse aggiuntive agli studenti in base ai loro bisogni educativi.
2. **Valutazione e Feedback**: L'IA non può sostituire la valutazione del docente, ma può essere utilizzata per fornire strumenti di monitoraggio continuo e feedback tempestivi su aree di miglioramento.
3. **Accessibilità**: Gli strumenti IA devono essere progettati e utilizzati per garantire che ogni studente, indipendentemente dalle sue capacità, possa beneficiare di una esperienza inclusiva.



Articolo 4 - Sistemi Ad Alto Rischio

1. **Sistemi di valutazione e orientamento**: Tutti i sistemi IA utilizzati per valutare o orientare gli studenti devono rispettare rigorosi standard di trasparenza, e essere sottoposti a **valutazione d'impatto**.
2. **Supervisione Umana**: Nessun sistema IA può prendere decisioni autonome riguardo la carriera scolastica o la valutazione finale degli studenti. Il personale scolastico deve

sempre essere coinvolto nelle decisioni importanti. Il personale deve verificare sempre l'accuratezza e l'attendibilità dei risultati generati.

3. **Tutela dei dati personali**: I dati sensibili degli studenti (es. risultati scolastici, informazioni sanitarie) devono essere trattati nel rispetto del **Regolamento Generale sulla Protezione dei Dati (GDPR)**.
4. **Trasparenza dei sistemi**: Ogni sistema IA utilizzato deve essere dotato di un'informativa chiara sulle modalità di raccolta, trattamento e conservazione dei dati. Inoltre per garantire trasparenza bisogna citare l'uso dell'IA nei documenti e materiali prodotti.
5. **Piattaforme consentite**: sono consentite piattaforme conformi al GDPR come Gemini, ChatGPT, Microsoft Copilot, Apple Intelligence, Samsung Intelligence. Le piattaforme devono garantire sicurezza, cifratura e opzioni per escludere l'uso dei dati a fini di training.
6. **Piattaforme vietate:** sono vietate piattaforme di paesi non conformi al GDPR o prive di adeguate garanzie.
7. - Prima di introdurre nuovi strumenti è obbligatoria la consultazione con il DPO.



Articolo 5 - Gestione dei Dati e Privacy

1. **Tutela dei dati personali**: I dati sensibili degli studenti (es. risultati scolastici, informazioni sanitarie) devono essere trattati nel rispetto del **Regolamento Generale sulla Protezione dei Dati (GDPR)**. Non inserire dati personali o sensibili reali nei sistemi IA.
2. **Trasparenza dei sistemi**: Ogni sistema IA utilizzato deve essere dotato di un'informativa chiara sulle modalità di raccolta, trattamento e conservazione dei dati.



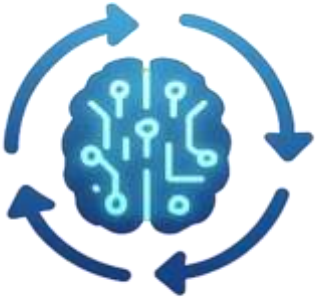
Articolo 6 - Formazione del Personale

1. **Formazione continua**: Tutti i membri del personale scolastico (docenti, dirigenti, amministrativi) devono essere formati sull'uso e sull'impatto dell'IA nel contesto educativo, nonché sui rischi legati all'IA e al GDPR.
2. **Aggiornamento professionale**: La scuola garantirà aggiornamenti periodici sulle tecnologie emergenti, sull'etica digitale e sulla gestione dei dati.



Articolo 7 - Coinvolgimento delle Famiglie e degli Studenti

1. **Informazione e Consenso**: Le famiglie e gli studenti saranno informati riguardo all'uso dell'IA a scuola. Il consenso informato sarà richiesto prima dell'utilizzo di sistemi che coinvolgano dati personali.
2. **Partecipazione attiva**: Gli studenti saranno coinvolti in attività di sensibilizzazione sull'uso etico e responsabile delle tecnologie digitali.



Articolo 8 - Monitoraggio e Revisione

1. **Valutazione periodica**: L'adozione dell'IA sarà monitorata periodicamente per valutarne l'efficacia, i benefici educativi e l'impatto sulle dinamiche scolastiche.
2. **Revisione continua**: Il regolamento potrà essere aggiornato in base all'evoluzione delle normative e delle tecnologie, nonché alle esigenze della comunità scolastica.

Articolo 9 - DPIA e governance

1. Per l'uso di IA in contesti a rischio è necessaria la Valutazione di Impatto sulla Protezione dei Dati (DPIA) e, se richiesto, la consultazione con il DPO.
2. - Ruoli e responsabilità sono definiti dal Dirigente scolastico in collaborazione con il DPO.

Articolo 10 - Sanzioni interne

1. L'uso non conforme può comportare misure correttive e disciplinari, nel rispetto del quadro contrattuale e delle procedure interne

RIFERIMENTI NORMATIVI
- Regolamento UE 2016/679 (GDPR)
- AI Act e Linee guida MIM 2025
- Linee guida internazionali su etica, DPIA e governance dell'IA in ambito educativo



Disposizioni per l'uso dei personal computer

1. Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività scolastica è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.

2. La Scuola rende noto che il personale incaricato che opera presso il servizio di assistenza informatica della stessa (nel seguito per brevità "Servizio IT") è composto da amministratore, tecnici, consulenti esterni e assistenti del team digitale. Il Servizio IT è autorizzato a compiere interventi nel sistema informatico della scuola, ognuno per la parte di propria competenza, al fine di garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici o manutentivi, quali, ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.

3. Ciascun dispositivo di proprietà della scuola è fornito di sistema operativo e applicazioni con licenza dell'Istituto o con licenza libera. Qualsiasi software aggiuntivo che si ritiene utile caricare sul dispositivo deve rispettare le leggi sul copyright.

4. Nessun utente può personalizzare i device in uso a più persone installando o rimuovendo applicazioni. In caso di sopravvenute particolari necessità contattare il team digitale e/o inoltrare richiesta al Dirigente Scolastico. L'inosservanza della presente disposizione espone La Scuola a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software, che impone la presenza nel sistema operativo dei dispositivi in uso di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico della Scuola, come disposta dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.

5. Le cartelle utenti presenti nei dispositivi di uso comune della Scuola sono aree di condivisione di informazioni e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività scolastica non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e backup da parte del personale del Servizio IT. Si ricorda che tutti i dischi o altre unità di memorizzazione locali - es. disco C: interno al PC - non sono soggette a manutenzione ordinaria da parte del personale incaricato del Servizio IT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

6. In caso di utilizzo di pc condivisi, si raccomanda di non salvare files con dati personali in aree del pc a cui possono accedere altri utilizzatori.

7. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna utilizzati, avvertendo immediatamente il personale del Servizio IT nel caso in cui siano rilevati virus.

8. Viene infine disposto il divieto di utilizzo per fini personali di strumenti della scuola, per spedire o per ricevere documentazione, e/o di fotocopiatrici della scuola, salva diversa esplicita autorizzazione da parte del Dirigente Scolastico o di un suo delegato.

9. Ogni Personal Computer in dotazione della scuola, sia ad uso didattico che di servizio in spazi comuni (laboratori, sala docenti, biblioteca…), deve essere spento ogni sera prima di lasciare i locali della Scuola. In caso di suo inutilizzo, il pc deve essere bloccato e l'utente si deve scollegare dal pc: lasciare un elaboratore incustodito, connesso alla rete, può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Disposizioni generali sulla dotazione ad uso didattico

1. Ogni classe è dotata di computer e di una LIM, monitor o schermo interattivo. L'uso del pc di classe e delle sue periferiche è ammesso solo agli insegnanti e concesso agli alunni solo in presenza degli stessi docenti.

2. Durante le ore di lezione, tutti i dispositivi tecnologici multimediali di proprietà o dati in dotazione alla classe devono essere tenuti normalmente spenti e saranno accesi per l'utilizzo secondo le indicazioni fornite dai docenti.

3. A sostegno della didattica, è ammesso l'uso dei dispositivi multimediali di proprietà della scuola o dei dispositivi portatili personali in classe, solo previa indicazione dei docenti che desiderino utilizzarli come strumenti integrativi della propria programmazione didattica; pertanto il loro utilizzo da parte degli studenti deve essere coerente con le richieste degli insegnanti. Tablet e pc portatili non devono essere usati fuori dalle aule e fuori dall'orario di studio.

4. Gli studenti sono autorizzati all'impiego dei dispositivi della scuola o dei loro personali solo ad uso didattico, ossia per la lettura e la consultazione dei loro e-book, per ricerche attraverso siti scolastici o dizionari on-line, oppure per lo svolgimento di test di apprendimento, sotto la supervisione degli insegnanti.

5. Ogni dispositivo di proprietà della scuola è riconducibile all'alunno al quale è stato assegnato tramite il codice identificativo numerico presente sul dispositivo: è pertanto vietato lo scambio del dispositivo con quello dei propri compagni e ogni studente può utilizzare esclusivamente quello a lui assegnato. Al termine dell'ora di laboratorio, sarà sua cura spegnere correttamente il device, eliminare il proprio account dalla macchina usata e consegnarlo al docente responsabile o riporlo adeguatamente nell'apposito carrello di caricamento.

6. Lo studente deve avere cura del dispositivo a lui dato in uso e di ulteriori strumentazioni o periferiche ad esso connesse (mouse, tastiera, tavolette grafiche, kit di robotica…) adottando tutte le necessarie cautele. Eventuali malfunzionamenti o danni rilevati vanno comunicati tempestivamente all'insegnante, che provvederà ad annotarlo e segnalarlo al membro del team digitale operante nel plesso.

7. Chi volontariamente o per negligenza procura un danno ad un qualsiasi dispositivo di proprietà della scuola, dato in dotazione o in uso temporaneo al singolo o alla classe, a o ad una delle sue parti, sarà sottoposto a sanzione disciplinare e dovrà risarcire il danno causato.

8. È vietato consumare cibi e bevande durante l'utilizzo dei dispositivi o nei pressi della postazione di lavoro. Gli studenti sono, inoltre, tenuti a igienizzare accuratamente le mani prima dell'utilizzo dei device di proprietà della scuola.

9. Per regolamentare l'uso dei dispositivi informatici ad uso didattico di proprietà della scuola, viene istituito un calendario digitale per la gestione delle prenotazioni, condiviso online dal team digitale con il gruppo docenti di ciascun plesso. I docenti sono tenuti a compilare il suddetto calendario preferibilmente entro il giorno lavorativo precedente l'effettivo utilizzo. In mancanza di altre prenotazioni, è consentito accedere alla strumentazione, previa registrazione, anche non avendone effettuata richiesta anticipata. L'uso va comunque sempre registrato al fine di un monitoraggio completo della strumentazione scolastica e di eventuali danni provocati dagli utenti.

Disposizioni sull'uso dei BYOD per il personale in servizio e gli studenti

Il termine "Bring your own device" (BYOD) - in italiano: "porta il tuo dispositivo" - è un'espressione usata per riferirsi alle politiche che permettono di portare i propri dispositivi personali a scuola e di usarli per avere gli accessi veloci alle informazioni scolastiche e alle loro applicazioni. L'Istituto Comprensivo autorizza l'utilizzo in ambito scolastico l'uso dei dispositivi di proprietà degli utenti, all'interno dei quali verranno quindi memorizzati dati e informazioni relative alle attività scolastiche, contenenti anche dati personali. Per essere autorizzato, tale utilizzo è tuttavia vincolato alle seguenti norme, che andranno scrupolosamente osservate.

1. Lo studente può, quotidianamente, portare a scuola il proprio dispositivo multimediale (tablet, ipad, notebook…), sprovvisto di scheda SIM e comunque offline, non connesso alla rete mobile, per la consultazione di libri in formato elettronico, sotto responsabilità delle famiglie per i danni accidentali e smarrimento. L'utilizzo in classe dei Byod è consentito esclusivamente durante le ore di lezione, ad esclusione dell'intervallo e del cambio d'ora, solamente per usi e scopi scolastici, sotto indicazione e vigilanza degli insegnanti.

2. Il personale che utilizzi, per le quotidiane esigenze di servizio, il proprio dispositivo è obbligato a dotare il device di proprietà di un dispositivo di protezione (PIN, impronta, ecc) ad esclusiva conoscenza del soggetto autorizzato, affinché le funzioni e i dati contenuti nell'account scolastico siano protetti da accessi da parte di terzi, a scuola e nella vita privata (famigliari, amici, ecc.).

3. Qualora il dispositivo venisse ceduto o dato in uso, anche temporaneo, a terzi, il soggetto autorizzato è tenuto a cancellare ed eliminare tutti gli accessi alla posta elettronica e ai dati personali. Il soggetto autorizzato sarà considerato responsabile civilmente e penalmente di quanto attribuito al proprio codice di accesso personale.

Disposizioni sull'uso degli smartphone e di altri dispositivi elettronici

1. È vietato l'utilizzo del telefono cellulare e di altri dispositivi elettronici (mp3, ipod, smartwatch ecc…) durante le attività scolastiche ed extrascolastiche pomeridiane, in tutti i locali della scuola. I dispositivi personali vanno tenuti spenti dall'inizio fino all'orario di termine delle lezioni, custoditi nello zaino o in contenitori comuni disposti nelle classi, sotto la responsabilità del docente in servizio, e comunque tenuti sempre disattivati durante la permanenza all'interno degli ambienti scolastici. Il mancato rispetto delle suddette regole sarà sanzionato.

2. È vietato l'uso dell'applicazione della fotocamera e dei registratori audio/video presenti sui dispositivi multimediali, se non espressamente autorizzato dall'insegnante. Non è ammesso l'uso di cellulari o di registratori per filmare o registrare lezioni. Eventuali fotografie o riprese fatte con gli smartphone o altri dispositivi elettronici all'interno della scuola e nelle sue pertinenze, senza il consenso scritto della/e persona/e riprese, si configurano come violazione della privacy e sono quindi perseguibili per legge, oltre ad essere sanzionate come previsto dal presente regolamento.

3. Si configurano come attività didattiche anche le uscite e i viaggi di istruzione, durante i quali l'uso del cellulare è consentito esclusivamente nei momenti e nelle modalità stabilite dagli accompagnatori.

4. In caso in cui l'alunno sia sorpreso ad usare il cellulare in tutti i casi non ammissibili ai sensi del presente regolamento, l'alunno sarà obbligato dal docente in servizio a spegnere il dispositivo.

5. Per quanto riguarda il personale docente e non docente, l'utilizzo di smartphone e altri dispositivi personali connessi alla rete è permesso in orario di servizio esclusivamente per motivi didattici o riconducibili al servizio, come la compilazione del registro elettronico.

Utilizzo e conservazione dei supporti rimovibili

1. È generalmente vietato, tranne in casi eccezionali come problemi alla rete internet, l'utilizzo di supporti rimovibili personali (chiavette USB, hard disk esterni…).

2. Tutti i supporti magnetici rimovibili (supporti USB, hard disk esterni, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how della scuola, devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. L'utente resta, in ogni caso, responsabile della custodia dei supporti e dei dati della scuola in essi contenuti; in particolare, i supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi.

3. Ogni dispositivo magnetico di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio IT.

4. In caso di smarrimento di una chiavetta USB contenente dati personali o altro dispositivo, è fatto obbligo di avvisare immediatamente il Dirigente scolastico e il Responsabile della protezione dei dati.

5. Ogni qualvolta si procederà alla dismissione di un personal computer l'Amministratore di Sistema provvederà alla distruzione o all'archiviazione protetta delle unità di memoria interne alla macchina stessa (hard-disk, memorie allo stato solido).

Utilizzo delle stampanti e dei materiali di consumo

1. L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti digitali come CD e DVD) è riservato esclusivamente ai compiti di natura strettamente istituzionale.

2. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

3. È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

Utilizzo delle password

Le password di ingresso alla rete, di accesso ai programmi e dello screensaver, sono previste ed attribuite dall'Incaricato della custodia delle Password, ovvero dal Dirigente Scolastico.

1. È necessario procedere alla modifica della password a cura dell'Amministratore di Sistema o dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni tre mesi (come previsto dal punto 5 del disciplinare tecnico allegato al Codice della Privacy, D.Lgs. n. 196/2003) con contestuale comunicazione all'Incaricato della custodia delle Password in busta chiusa.

2. La comunicazione di variazione delle password dovrà essere consegnata al Dirigente Scolastico in busta chiusa, con data e firma dell'incaricato apposte sul lembo di chiusura.

3. Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

4. La password deve essere immediatamente sostituita, dandone comunicazione scritta all'Incaricato della custodia delle password, nel caso si sospetti che la stessa abbia perso la segretezza.

5. Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia, per iscritto, al Titolare.

Disposizioni per la connessione e l'utilizzo della rete internet

1. L'Istituto Comprensivo dispone di connessione alla rete internet a banda larga in fibra ottica di Lepida in tutti i plessi scolastici. La velocità di download, così come quella di upload, arrivano fino a 1Gbps, garantendo un adeguato servizio, sia per la didattica che per le attività di segreteria. La configurazione del firewall perimetrale è affidata ad una società di consulenza esterna. Sono attivi di default i blocchi dei servizi peer to peer e i filtri di base, mentre si provvede continuamente ad implementare i web filters relativi ai contenuti accessibili.

2. L'utilizzo dei dispositivi multimediali a scuola avviene attraverso la connessione alla rete wi-fi dell'Istituto o tramite cavo ethernet in spazi cablati in cui il segnale wireless non risulta performante. Tutti i device sono già configurati per l'utilizzo della rete. Ogni tentativo di manomettere la rete dell'Istituto sarà sanzionato come grave infrazione disciplinare.

3. All'interno della scuola, la rete internet è area di comunicazione finalizzata ad uso strettamente didattico e non può essere utilizzata per scopi diversi. Non è consentito agli studenti utilizzare in classe strumenti per la navigazione in internet diversi dalla rete wi-fi dell'Istituto e non è consentito in alcun modo navigare in internet senza il permesso dei docenti e la loro diretta sorveglianza.

4. È possibile entrare nella rete e nei programmi esclusivamente utilizzando il proprio account istituzionale o con altro account istituzionale indicato dal docente.

5. È assolutamente proibito entrare nella rete e nei programmi con credenziali di autenticazione diverse da quelle assegnate. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

6. È proibito utilizzare i social network per uso personale. Qualunque uso della connessione che violi le leggi civili e penali in merito è vietato e saranno sanzionati utilizzi non conformi alle disposizioni del presente regolamento.

7. Non è consentito a nessuno il download e la memorizzazione su dispositivi multimediali per uso scolastico di materiali di natura oscena, oltraggiosa e/o discriminatoria. L'utente sarà ritenuto personalmente responsabile del materiale prodotto o visionato, dei danni eventualmente causati a terzi e delle violazioni di legge effettuate tramite l'utilizzo del proprio dispositivo o di quello a lui dato in uso. Nel caso di studenti, il responsabile del servizio informatico della scuola e i docenti hanno la facoltà, in qualunque momento, di accedere al dispositivo e ai dati trattati, comprese le navigazioni web e altri archivi. Nell'immediato si procederà alla rimozione di file e applicazioni ritenuti pericolosi per la sicurezza, e la trasgressione sarà sanzionata ai sensi del presente regolamento.

8. Nel caso di comparsa sul dispositivo di messaggi, informazioni o pagine che creino disagio e/o in generale nel caso di malfunzionamenti del dispositivo o del sistema, gli studenti sono tenuti ad informare immediatamente gli insegnanti.

Navigazione in Internet e WiFi

1. Durante l'utilizzo di internet all'interno della scuola è assolutamente proibita la navigazione per motivi diversi da quelli strettamente legati all'attività scolastica, sia con strumenti scolastici che personali. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

● l'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività scolastica e previa verifica dell'attendibilità dei siti in questione;

● l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili, fatti salvi i casi direttamente autorizzati dalla Dirigenza (o eventualmente dal Responsabile d'ufficio e/o del Servizio IT) e comunque nel rispetto delle normali procedure di acquisto;

● effettuazione di operazioni quali prenotazioni o consultazione referti medici su portali inerenti la salute;

● ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività scolastica (ad esempio e-commerce);

● l'iscrizione con account della scuola e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche, forum, blog, ecc.. anche utilizzando pseudonimi (o nickname);

● collegamenti a servizi P2P (torrent, e-mule, file sharing) o lo scaricamento di contenuti multimediali per finalità ludiche;

● sono altresì vietati collegamenti a siti di gioco online.

2. L'utilizzo di tutte le reti WiFi presenti presso la Scuola è limitato agli utenti autorizzati. A tale scopo si precisa che l'utilizzo di qualsiasi rete WiFi disponibile è possibile solo tramite la digitazione di una password di accesso, unica per ciascun plesso. È assolutamente vietato comunicare a studenti o terzi non autorizzati e non facenti parte della comunità scolastica la password o le credenziali di accesso alle reti WiFi scolastiche. Si rende altresì noto che tutti i dispositivi didattici sono già configurati per l'accesso alla rete dell'Istituto.

3. Non è consentito l'accesso a siti e servizi che prevedano un traffico di dati sulla rete tali da pregiudicare il buon funzionamento della medesima. Durante l'utilizzo della rete Internet è vietato:

● svolgere qualunque attività che sia in contrasto con la normativa italiana ed europea;

● accedere a siti che per contenuti ed immagini siano in contrasto con le finalità servizio e/o illegali (siti pedofili, pornografici, che ispirano alla violenza, al razzismo, ecc.);

● inviare messaggi di posta secondo modalità indiscriminate (spamming);

● svolgere qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno esterno pubblico o privato;

● usare meccanismi o strumenti di qualsiasi natura atti ad eludere i sistemi di protezione da copia abusiva del software, a rivelare password, ad identificare eventuali vulnerabilità della sicurezza dei vari sistemi, a decriptare file crittografati o a compromettere la sicurezza della rete in qualsiasi modo.

4. L'utente, personale in servizio o studente, è direttamente responsabile delle attività svolte durante la connessione a Internet: le conseguenze penali e civili derivanti da un uso fraudolento della medesima rete e ogni responsabilità civile e penale è in capo ai singoli utilizzatori della rete Internet. In caso di alunni, l'infrazione sarà sanzionata ai sensi del presente regolamento.

Utilizzo della posta elettronica

La casella di posta elettronica assegnata all'utente è uno strumento da utilizzarsi solo per le attività scolastiche. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

1. L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività scolastica o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione. L'utilizzo di caselle di posta elettronica personali è di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale.

2. L'utente è responsabile del contenuto dei messaggi inviati. Ciascun messaggio in uscita deve consentire l'identificazione univoca del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.

3. È fatto divieto di utilizzare le caselle di posta elettronica della scuola per motivi diversi da quelli strettamente legati all'attività scolastica. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

● l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali non legati all'attività scolastica;

● l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list, offerte di siti e-commerce, newsletter non pertinenti con le attività legate al servizio;

● la partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo, lo si dovrebbe comunicare immediatamente al personale del Servizio IT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

4. È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.

5. È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web non conosciuti).

6. L’indirizzo e-mail è un dato personale e non va rivelato ad alcuno se non necessario: in caso di invio di comunicazioni e/o circolari per e-mail non si devono quindi mettere gli indirizzi e-mail dei destinatari in chiaro nel campo CC, ma invece nel campo CCN, in modo che non siano visibili agli altri.

Utilizzo del Registro elettronico e altre piattaforme digitali scolastiche

L’utente è tenuto a osservare le specifiche disposizioni relative alla tutela della privacy anche nell'utilizzo del registro elettronico e delle piattaforme didattiche digitali a cui ha ottenuto accesso. Per queste ultime si rimanda alla Guida di Utilizzo ai Servizi di Google Workspace for Education per tutte le norme di comportamento relative all’utilizzo del servizio.

- **Accesso e Finalità:** L’Istituto, coerentemente con il PTOF, fornisce agli studenti account personali per l'accesso ai servizi Google Workspace for Education.
- **Limitazioni Tecniche:** Per gli studenti minori di 14 anni, l’accesso diretto a Gemini tramite account istituzionale è inibito in via predefinita dall’Amministratore di sistema, garantendo così la tutela del minore e l’adesione alle policy di sicurezza di Google.
- **Uso Didattico Guidato:** Eventuali attività didattiche che prevedano l’utilizzo dell’IA per le classi della scuola secondaria di primo grado potranno avvenire solo sotto la **supervisione diretta del docente**. Quest'ultimo utilizzerà il proprio account in modalità collettiva (es. proiezione sulla LIM), assicurando che non avvenga alcuna profilazione o trattamento di dati personali degli studenti all'interno dei motori di intelligenza artificiale.

Partecipazioni a social media

L’utilizzo dei social media ufficiali della Scuola verrà gestito ed organizzato esclusivamente dalla Dirigenza attraverso specifiche direttive ed istruzioni operative rivolte al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti. Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, la Scuola ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio della scuola, anche immateriale, quanto i propri collaboratori e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media. La policy qui dettata deve venir seguita dagli utenti, sia che utilizzino dispositivi messi a disposizione dal Titolare, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali. Le medesime indicazioni sono valide anche per gli alunni, per la partecipazione a social media non moderati dal personale scolastico.

1. La condivisione dei contenuti nei social media deve sempre rispettare e garantire i diritti dei soggetti coinvolti. Ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d’autore, sia di terzi che della Scuola.

2. L’utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi, collaboratori della scuola e di studenti, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all’interno dei luoghi della scuola, se non con il preventivo consenso della Dirigenza.

3. L’utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso la Scuola, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie.

4. Nell'utilizzo dei propri account di social media, l'utente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente all'istituzione

Scolastica di appartenenza. In ogni caso, l'utente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.

5. Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'amministrazione e in difformità alle disposizioni di cui al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità attribuibili direttamente alla pubblica amministrazione di appartenenza.

Disposizioni a tutela della privacy

1. La riservatezza dei dati personali è un valore per l'Istituto Scolastico ed occorre quindi che tutti gli attori, interni ed esterni, siano consapevoli che è vietato comunicare ad estranei contatti e altri dati patrimonio della scuola. È obbligatorio pertanto attenersi alle disposizioni in materia di Privacy e di misure adeguate di sicurezza dei dati personali.

2. L'accesso alle piattaforme didattiche dell'istituto deve essere consentito esclusivamente previa autenticazione informatica. A ciascun utente sono fornite credenziali per l'accesso alla rete e al proprio account. Le password per l'accesso alla rete, ai programmi e al proprio profilo digitale non possono essere divulgate e devono essere custodite con la dovuta diligenza.

3. È fatto obbligo a ciascun utente di effettuare la disconnessione dal proprio account dalle pagine web consultate con il proprio profilo (ad esempio registro elettronico, siti delle case editrici…) e comunque al termine di ogni sessione di lavoro, al fine di custodire i propri dati sensibili e quelli di terzi eventualmente presenti in documenti di staff.

4. É fatto obbligo agli studenti di effettuare la rimozione del proprio profilo account dalle macchine chromebook date in dotazione per sessioni di lavoro in classe.

5. Si ricorda che, quando si utilizza un dispositivo condiviso con altri utenti, non si deve mai memorizzare su di esso alcuna password, quali ad esempio quelle del registro elettronico o dell'account Google: memorizzando la password, altri utenti potrebbero facilmente accedere ai dati personali dell'utente loggato. L'uso dei dispositivi comuni deve essere pertanto attuato nel rispetto della privacy degli utenti, utilizzando l'accesso come ospite o con finestra in incognito o avendo cura di rimuovere il proprio profilo chrome su pc in uso a più utenti.

6. È vietato salvare sui dispositivi comuni documenti privati o contenenti dati sensibili di terzi. Al termine di ogni sessione di lavoro è fatto obbligo di pulire la cartella download ed eliminare definitivamente i file di propria proprietà, ovvero di eliminare il proprio account.

7. È vietato salvare sul personal computer e sul server della scuola, per scopi personali, file contenenti dati ritenuti sensibili, quali ad esempio copie delle buste paga (dipendenti) o altri dati sensibili quali esami, visite mediche, verbali di riunioni quali consigli di classe o interclasse, ecc. in qualsiasi formato. Qualora fossero rinvenuti file in particolare recanti dati sensibili di terzi, il personale del Servizio IT può, in qualunque momento e senza preavviso alcuno, procedere alla rimozione dal dispositivo.

Disposizioni a tutela della proprietà intellettuale

1. Tutti gli utenti sono tenuti a rispettare le regole di correttezza e riservatezza in campo telematico, nonché eventuali implicazioni riguardanti la proprietà intellettuale del materiale utilizzato.

2. È vietata la diffusione del materiale didattico per il quale vi è diritto di proprietà della scuola o dei singoli docenti sul sito della scuola o sulle piattaforme social media a cui la scuola partecipa, se non dietro esplicita autorizzazione del Dirigente e del diretto interessato.

Responsabilità

1. È fondamentale che tutti gli utenti siano pienamente consapevoli dei rischi a cui si espongono durante l'utilizzo dei dispositivi dell'istituto. I genitori si impegnano a collaborare con la scuola affinché vengano rispettate le norme previste dal presente regolamento tramite una assunzione di responsabilità condivisa con i propri figli, rilasciata attraverso apposita dichiarazione.

2. Nelle sessioni di lavoro in classe per attività didattiche ed extradidattiche, i docenti sono responsabili dell'utilizzo dei dispositivi informatici e hanno l'obbligo di sorvegliare e responsabilizzare gli studenti e le studentesse rispetto ad un uso consapevole e sicuro.

3. Gli utenti non devono lasciare incustoditi i dispositivi informatici, vigilare per evitare danneggiamento della dotazione tecnologica di Istituto data in uso e devono provvedere, al termine dell'utilizzo, a riporre la strumentazione nelle stesse condizioni in cui l'hanno trovata.

4. Le violazioni al presente Regolamento e gli utilizzi impropri dei dispositivi multimediali e della rete saranno segnalati e sanzionati dall'Istituto. In caso di violazione da parte degli alunni, i docenti provvederanno a segnalare l'accaduto con immediata annotazione sul registro elettronico e successiva comunicazione ai genitori. Eventuali altri provvedimenti disciplinari saranno stabiliti dai singoli Consigli di Classe secondo la gravità del caso e in coerenza con le disposizioni del presente regolamento.

Sanzioni

1. In caso di reiterata infrazione delle norme del regolamento, previa comunicazione alla famiglia dell'alunno/a e dopo la convocazione del Consiglio di Classe straordinario, sarà comunicata la sanzione disciplinare di sospensione fino a tre giorni, anche con eventuale obbligo di frequenza.

2. In caso di utilizzo dei dispositivi elettronici per registrazione di immagini o audio e loro successiva diffusione non autorizzata sui social, fatto l'obbligo di rimozione immediata del materiale pubblicato, è previsto l'allontanamento del trasgressore dalla comunità scolastica da 7 fino a 15 giorni, con o senza obbligo di frequenza, ed eventuale esclusione dalla partecipazione ai viaggi d'istruzione e/o uscite didattiche, secondo la gravità del caso e danno arrecato a terzi coinvolti.

3. Se l'infrazione si dovesse configurare come atto di cyberbullismo, l'Istituto Comprensivo si riserva la facoltà di segnalare alle autorità competenti l'accaduto, per gli opportuni accertamenti ed i provvedimenti del caso, in ottemperanza a quanto disposto dalle leggi e regolamenti vigenti. Per le sanzioni di questa fattispecie, si faccia riferimento al Regolamento per l'individuazione e il contrasto dei fenomeni di bullismo, cyber-bullismo e vittimizzazione vigente nella nostra Scuola.

4. In caso di infrazioni da parte del personale, la sanzione sarà comminata in relazione alla gravità del fatto rilevato. A

Accesso ai dati trattati dall'utente

Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi della scuola (ad esempio, verifica costi di connessione a Internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività degli

utenti, è facoltà della Direzione della scuola, tramite il personale del Servizio IT, accedere direttamente e in qualsiasi momento, senza alcun preavviso, nel rispetto della normativa sulla privacy e delle procedure, a tutti gli strumenti informatici della scuola e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

Amministratore di sistema

L'Amministratore di Sistema è il soggetto cui è conferito il compito di sovrintendere alle risorse informatiche dell'Istituto e a cui sono consentite in maniera esclusiva le seguenti attività:

1. gestire l'hardware e il software di tutte le strutture tecniche informatiche di appartenenza dell'Istituto, collegate in rete o meno;

2. gestire esecutivamente (creazione, attivazione, disattivazione e tutte le relative attività amministrative) gli account di rete e i relativi privilegi di accesso alle risorse, assegnati agli utenti della Rete Informatica istituzionale, secondo le direttive impartite dal Dirigente Scolastico;

3. monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

4. creare, modificare, rimuovere o utilizzare qualunque account o privilegio con l'autorizzazione del Dirigente Scolastico, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

5. rimuovere programmi software dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

6. rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

7. utilizzare le credenziali di accesso di amministrazione del sistema, o l'account di un utente tramite reinizializzazione della relativa password, per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale utilizzo deve essere esplicitamente richiesto dal Titolare per l'utente assente o impedito, e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

Utilizzo laboratori di informatica

1. Le chiavi dei laboratori digitali (laboratori di informatica) vanno custodite dal DSGA. Il ritiro e la riconsegna delle chiavi sono di competenza del docente che utilizza il laboratorio.

2. L'insegnante avrà cura, all'inizio ed alla fine di ogni lezione, di verificare l'integrità di ogni singola postazione e di ogni singolo strumento utilizzato.

3. Ogni alunno deve segnalare all'insegnante eventuali anomalie o danni riscontrati alle postazioni, il quale lo riferirà a sua volta al responsabile di laboratorio.

4. L'insegnante, qualora alla fine della lezione dovesse rilevare danni, manomissioni alle attrezzature è

tenuto a darne tempestiva comunicazione al Dirigente Scolastico e al DSGA.

5. É assolutamente proibito scollegare i cavi di alimentazione ed i cavi di rete dei PC presenti.

6. É proibito alterare le configurazioni del desktop e modificare le impostazioni del sistema operativo.

7. Le pen-drive portate da casa possono essere utilizzate solo sotto la supervisione dell'insegnante che attuerà le procedure di controllo per verificare l'assenza di virus.

8. Al termine del lavoro ogni alunno deve chiudere le applicazioni che ha utilizzato e lasciare l'aula e le attrezzature in ordine.

9. Dopo la lezione l'insegnante deve controllare che tutto venga lasciato in ordine.

10. L'aula non può essere utilizzata per scopi diversi da quelli a cui è destinata.

11. L'accesso delle classi ai laboratori deve essere regolamentato dall'osservanza della tabella oraria compilata da tutti i docenti interessati all'utilizzo dei PC o di altra strumentazione.

12. È assolutamente proibito l'accesso degli alunni nell'aula di informatica in assenza dell'insegnante.

13. La classe deve mantenere un comportamento corretto per evitare eventuali danni alle strutture che ha in uso.

14. L'utilizzo dei laboratori di informatica comporta la puntuale compilazione del registro delle presenze, sul quale è obbligatorio annotare eventuali anomalie/malfunzionamenti dei dispositivi hardware e dei software.

15. É vietato introdurre bevande all'interno dei laboratori di informatica durante l'utilizzo dei computer o/e delle stampanti.