REGOLAMENTO INFORMATICO
LICEO GINNASIO STATALE "GIORGIONE"

Disciplinare interno ai sensi del Provvedimento Garante n. 13/07 del 1° marzo 2007

Aggiornamento del Regolamento informatico approvato dal Consiglio di Istituto con delibera n. 26 del 30/06/2023

INDICE

1 SCOPO E AMBITO DI APPLICAZIONE

Il nostro Istituto, da anni è fortemente impegnato nell'attuazione del PNSD ("*Piano Nazionale Scuola Digitale*"), investendo in infrastrutture, sperimentando nuove metodologie didattiche e impegnandosi in un percorso continuo di formazione del personale docente ed amministrativo.

Nonostante l'Istituto risulti articolato su quattro distinti plessi, ogni sede è dotata di collegamento Internet e rete Wi-fi. Ogni aula è attrezzata con Digital Board, o LIM, pc e video proiettore.

Da anni ormai è stato adottato il registro elettronico e, da subito, tutti i docenti sono stati dotati di tablet acquistati con risorse di bilancio e dati in uso ad ogni inizio di anno scolastico. Rientra nella facoltà degli insegnanti utilizzare i propri supporti o postazioni fisse dell'Istituto considerando che tutte le aule sono dotate di pc con collegamento alla Rete.

Oltre alle dotazioni digitali, multimediali e di rete presenti negli altri laboratori, nelle aule speciali e nelle aule didattiche, l'Istituto dispone di moderni laboratori informatici:

- multimediale;
- linguistico;
- tecnologie musicali.

Tali laboratori risultano indispensabili considerando che il Liceo Giorgione, oltre agli indirizzi tradizionali comprende le scienze applicate, il linguistico e il musicale. Per quest'ultimo è stato utilizzato il finanziamento di apposito progetto PON, che ha consentito la realizzazione di un moderno e attrezzato laboratorio per lo studio della disciplina delle "Tecnologie Musicali" ove, oltre all'impiego nelle materie classiche si produce e si registra musica.

Da qualche anno, inoltre, l'Istituto si è dotato di tre laboratori mobili che consentono di operare all'interno dell'aula, considerato che il carrello, oltre ad essere attrezzato sul piano della connessione con l'unità centrale del docente, è dotato di tablet che fungono da pc.

Nei passati anni scolastici sono state attuate delle sperimentazioni "classe digitale", che hanno visto coinvolte, in tempi diversi, il percorso del triennio di tre classi dello scientifico ordinario, all'interno di aule adeguatamente attrezzate.

Le nuove tecnologie costituiscono, però anche una potenziale fonte di rischi.

Scopo del presente documento vuole essere disciplinare l'utilizzo delle postazioni di lavoro da parte del personale utente del Liceo Giorgione. Le indicazioni contenute in questo documento dovranno essere applicate per un corretto utilizzo delle risorse informatiche messe a disposizione per lo svolgimento delle relative attività.

1.1 PRINCIPI GENERALI

Nell'impartire le seguenti prescrizioni il Liceo Giorgione tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia. Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica. I trattamenti rispettano le garanzie in materia di protezione dei dati e si svolgono nell'osservanza dei principi di necessità, correttezza, per finalità determinate, esplicite e legittime, osservando il principio di pertinenza e non eccedenza e nella misura meno invasiva possibile.

2 DESTINATARI

Destinatari del presente documento sono da considerarsi tutti coloro che utilizzano postazioni informatizzate all'interno dell'Istituto (di seguito anche "Utenti") e, in particolare, il personale del Liceo Giorgione dotato di

una stazione di lavoro informatizzata. A tal fine, il termine "personale" è da intendersi in senso ampio: Dirigente Scolastico, Dsga, docenti, amministrativi, tecnici e collaboratori scolastici.

3 DESCRIZIONE DEL DOCUMENTO

Le norme che seguiranno richiamano gli utenti a un uso corretto e generalizzato delle infrastrutture di rete (interna ed eventuale esterna), il cui uso improprio può generare problemi, nonché difficoltà di utilizzo delle macchine, con possibili danni al loro funzionamento e connessi danni di natura economica.

Le risorse, hardware e software, in dotazione al personale del Liceo Giorgione, quali personal computer, notebook, tablet, stampanti, scanner, applicazioni gestionali, software di base, strumenti di sviluppo, programmi di utilità, ecc. (d'ora in avanti "dispositivi informatici") costituiscono un valore per il Liceo Giorgione e come tali devono essere adeguatamente protette.

Al fine di ridurre al minimo i rischi di indisponibilità, accesso non autorizzato, distruzione o perdita, anche accidentale, di informazioni il Liceo Giorgione ha definito:

- linee di comportamento atte a impedire il presentarsi di problemi e/o minacce alla sicurezza nel trattamento dei dati
- regole per l'accesso, l'utilizzo e la protezione delle proprie risorse informatiche da parte del personale del Liceo Giorgione

L'utilizzo improprio della postazione informatica e/o l'introduzione di software diverso da quello fornito ed installato dal personale autorizzato dal Liceo Giorgione, potrebbe compromettere il corretto funzionamento dei beni informatici e arrecare danni quali accessi abusivi, virus informatici, trattamento illecito, sia alle apparecchiature in dotazione sia alla rete del Liceo Giorgione.

Gli utenti hanno diritto di accedere alle risorse informatiche per le quali sono stati espressamente autorizzati e di utilizzarle esclusivamente per gli scopi inerenti alle mansioni svolte.

Pertanto, ogni soggetto è tenuto a:

- adottare, nell'ambito delle proprie attività, tutte le misure di sicurezza atte a prevenire la possibilità di accessi non autorizzati, furti, frodi, danneggiamenti, distruzioni o altri abusi nei confronti delle risorse informatiche
- attuare le suddette prescrizioni, anche attraverso l'adozione delle modalità d'utilizzo riportate nel presente documento, nonché a segnalare eventuali violazioni alle medesime o situazioni che possano presentare dubbi relativamente alla sicurezza delle informazioni trattate.

4 LINEE GUIDA PER L'USO DEI DISPOSITIVI INFORMATICI

I dispositivi informatici (vedi par. 3) affidati all'utente sono strumenti di lavoro e ogni utilizzo non inerente all'attività lavorativa può generare disservizi e costi di manutenzione; pertanto, gli utenti devono essere consapevoli delle loro specifiche responsabilità nella custodia e nel corretto utilizzo della propria stazione di lavoro**. In particolare, si ricorda che ai sensi della vigente normativa in tema di tutela dei dati personali (Reg. UE 2016/679) gli incaricati ("autorizzati") del trattamento sono tenuti all'applicazione delle istruzioni impartite dal titolare.**

4.1 CUSTODIA DELLA POSTAZIONE DI LAVORO

L'utente è direttamente responsabile dei dispositivi informatici a lui assegnati, pertanto:

- deve attivare manualmente lo screen saver in caso di assenza temporanea dall'ufficio attraverso la pressione simultanea dei tasti CTRL-ALT-CANC e la selezione dell'opzione "Blocca Computer", al fine di impedire durante l'assenza l'accesso alle applicazioni da parte di personale non autorizzato

- non deve modificare le caratteristiche impostate sul proprio PC. È vietato installare software, sia esso freeware o di pubblico dominio, dispositivi quali modem e/o router esterni, chiavette per la navigazione Internet non previste nella configurazione standard del personal computer assegnato.

Oltre a quanto fin qui riportato, per eventuali dispositivi mobili (es. notebook, tablet, iPad ecc.) devono essere prese ulteriori misure cautelative al fine di custodirli con diligenza. È buona regola adottare ogni misura idonea a prevenire la sottrazione del dispositivo mobile o di parte di accessori del medesimo anche quando vengono lasciati all'interno dei locali dell'Istituto e non ed evitare di lasciare, anche solo temporaneamente, i dispositivi mobili incustoditi. In caso di furto o smarrimento di dispositivi informatici dotati di collegamento alla rete Liceo Giorgione l'utente deve immediatamente avvisare l'amministratore di sistema, che attuerà i provvedimenti cautelativi del caso.

4.2 ACCESSO ALLE RISORSE INFORMATICHE

Gli strumenti adottati dal Liceo Giorgione per l'accesso alle risorse informatiche (es. codici di accesso, user-id,) sono di uso strettamente personale e l'utente è tenuto a custodirli in modo appropriato.

Gli accessi alla rete Liceo Giorgione, alla posta elettronica, al sistema di archiviazione della mail e in generale a tutte le applicazioni sono regolati da uno o più set di credenziali individuali (composti da una username e una password), le quali dovranno essere custodite dal personale del Liceo Giorgione con la massima diligenza e non divulgate.

A fronte di problemi di accesso alle postazioni di lavoro riconducibili a un errato inserimento della password, sia esso dovuto a incuria nella digitazione o dimenticanza della stessa, che causano un blocco dell'account, si rimanda al paragrafo 5 ove viene specificata la corretta procedura da utilizzare dagli utenti per la richiesta di assistenza IT al personale autorizzato dal Liceo Giorgione.

Gli utenti sono tenuti a seguire le seguenti istruzioni:

- al termine di qualunque sessione riservata di lavoro o di assenza temporanea è obbligatorio uscire dall'account o bloccare il computer.
- Non spegnere mai il PC mentre è in esecuzione un aggiornamento. Al termine dell'istallazione il computer si spegnerà automaticamente.
- È vietato modificare le caratteristiche impostate sui Pc, salvo con autorizzazione esplicita dell'assistente tecnico informatico oppure dell'Amministratore di sistema.
- Non è possibile eseguire operazioni di manutenzione ordinaria o straordinaria autonomamente. È vietato inserire password locali alle risorse informatiche assegnate (come, ad esempio, password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e dovutamente comunicate agli amministratori di sistema;
- per conservare i dati inerenti alla propria attività lavorativa dovranno essere utilizzate le cartelle di rete messa a disposizione, siano esse ad accesso condiviso (share di gruppo) o esclusivo (share ad accesso riservato del singolo utente);
- non è consentito avere sulla propria postazione e/o su share di rete materiale in formato elettronico di carattere personale (foto, documenti non attinenti alla mansione svolta, film, musica)

4.3 REGOLE PER STUDENTI E LABORATORI

Per i laboratori, gli utenti sono tenuti a seguire le seguenti istruzioni:

- I docenti che accederanno ai laboratori dovranno firmare l'ora d'ingresso e l'ora di uscita.
- Non è possibile rimuovere dall'aula il materiale in esso presente, senza autorizzazione del Dirigente Scolastico.
- Il materiale dovrà essere lasciato in ordine dove è stato trovato.

- Chiunque prenda uno strumento digitale in consegna dovrà registrare su apposito libro l'ora in cui ne viene in possesso, l'ora in cui lo restituisce ed eventuali anomalie.
- Ogni notebook e il relativo cavo di alimentazione saranno provvisti di etichetta del medesimo colore per contraddistinguerli e riconoscerli.
- Il personal computer deve essere spento (schermo compreso) al termine dell'orario delle lezioni o di servizio, comunque prima di lasciare i laboratori di informatica. 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.
- Eventuali guasti, rotture o ammanchi devono essere segnalati da parte del docente responsabile sull'apposito "registro guasti" presente all'interno dei laboratori. L'assistente tecnico provvederà alla corretta gestione del malfunzionamento, per consentire gli interventi necessari (come da apposito registro). Per quanto riguarda eventuali guasti dei dispositivi presenti all'interno delle aule, questi dovranno essere portati prontamente all'attenzione del personale Tecnico al massimo alla fine della lezione.
- Non è possibile rimuovere dall'aula il materiale in esso presente, senza autorizzazione del Dirigente Scolastico.
- Il docente dell'ultima ora provvede a ritirare ed eventualmente ricollocare nell'apposita posizione il materiale utilizzato.
- La strumentazione fornita in dotazione deve essere riconsegnata integra alla fine delle attività previste, in accordo con i docenti del C.d.C., nel caso dello studente, e col Dirigente Scolastico, nel caso del personale della scuola.
- Gli utenti sono responsabili di rotture e/o disfunzioni delle attrezzature causate da scorretto utilizzo delle stesse. Coloro che provocano dolosamente o colposamente danni alle attrezzature e/o apparecchiature, dell'aula o del laboratorio sono soggetti a sanzioni disciplinari, nel caso dello studente, e sono tenuti al risarcimento del danno.
- Ogni autorizzazione concessa allo studente, relativa alla gestione del dispositivo personale, deve essere registrata sulla scheda dello stesso.

Si ricorda, inoltre, che il Garante Privacy ha emesso il 10 giugno 2010 un vademecum per la sicurezza e la privacy nelle scuole, mentre dal 6 settembre 2012 vige un memorandum contenente le indicazioni inerenti all'utilizzo di tablet, smartphone, pc, ecc. In particolare, il Garante ricorda l'uso strettamente personale degli smartphone, nel rispetto della persona e che ogni Istituto scolastico decide nella propria autonomia (si veda il Regolamento di Istituto per ciò che concerne la regolamentazione dell'uso di cellulari e tablet). Comunque, sottolinea che non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. Si ricorda che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie nonché in responsabilità civile e penale. Le stesse cautele valgono per l'uso dei tablet, se adoperati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi online (documento emanato il 6 settembre 2012).
Infine, si rammenta agli studenti che: "…*va prestata particolare attenzione all' eventuale pubblicazione delle immagini su Internet, e sui social network in particolare. In caso di comunicazione sistematica o diffusione, diventa infatti necessario di regola ottenere il consenso delle persone presenti nelle fotografie e nei video. È possibile registrare la lezione esclusivamente per scopi personali, ad esempio per motivi di studio individuale. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente*

tutte le persone coinvolte nella registrazione e ottenere il loro esplicito consenso. Nell'ambito dell'autonomia scolastica, gli istituti possono decidere di regolamentare diversamente o anche di inibire apparecchi in grado di registrare. Le istituzioni scolastiche hanno, comunque, la possibilità di regolare o di inibire l'utilizzo di registratori audio-video, inclusi i telefoni cellulari abilitati, all'interno delle aule di lezione o nelle scuole stesse. Non è possibile, in ogni caso, diffondere o comunicare sistematicamente i dati personali di altre persone (ad esempio immagini o registrazioni audio/video) senza aver prima informato adeguatamente le persone coinvolte e averne ottenuto l'esplicito consenso" (Documento del 10 luglio 2010). Nella fattispecie il Liceo Giorgione riferisce gli usi degli strumenti digitali, dei device di qualsiasi genere, dei software e delle reti a quanto consentito nel Regolamento d'Istituto, con particolare riguardo all'Art. 30bis e con le modalità ivi indicate.

4.4 UTILIZZO DEL SOFTWARE

Non è consentito l'uso di programmi diversi da quelli distribuiti e installati ufficialmente dalle strutture preposte, così come non è consentito installare autonomamente programmi. Eventuali richieste di installazione devono essere inoltrate all'amministratore di sistema, che vaglierà la fattibilità e nel caso provvederà a installare quanto richiesto (si rimanda al paragrafo 5 per un maggior dettaglio inerente alle modalità di richiesta).

L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre il Liceo Giorgione a gravi responsabilità civili e penali in caso di violazione della normativa a tutela dei diritti d'autore sul software.

A tal proposito, il Liceo Giorgione effettua periodici controlli sui dispositivi informatici volti a rilevare l'eventuale presenza di software non autorizzato. Tale attività non prevede in nessun caso il monitoraggio, neppure preterintenzionale, delle attività del prestatore di lavoro o del contenuto di dati personali nel PC.

4.5 UTILIZZO DI DISPOSITIVI ESTERNI

Laddove si renda necessario l'utilizzo di dispositivi quali chiavi USB, hard disk esterni, supporti ottici, schede di memoria SD/xD/CF… ecc. devono essere autorizzati, richiesti e acquistati secondo le procedure in essere del Liceo Giorgione.

4.6 PREVENZIONE DEI VIRUS INFORMATICI

Ogni personal computer affidato agli utenti è dotato di un software antivirus centralizzato ad aggiornamento automatico al fine di prevenire l'introduzione di virus informatici che possano compromettere l'integrità del software e delle stazioni di lavoro.

L'utente deve sempre tenere conto del fatto che il programma antivirus non fornisce una protezione assoluta e in particolare tra due aggiornamenti consecutivi esiste una finestra temporale di rischio entro la quale si possono introdurre virus non ancora noti dal programma stesso.

Pertanto, sarà cura dell'utente rispettare le seguenti linee guida:

- mantenere la configurazione del sistema operativo in modo da permettere la visualizzazione dell'estensione dei file. Tale accorgimento rende più difficile il mascheramento da parte di file potenzialmente pericolosi (programmi EXE e script di vario tipo) che impiegano estensioni doppie (es. "leggimi.txt.vbs" oppure logo.jpg.exe");
- è fatto divieto disabilitare o disattivare i servizi relativi al software dell'Anti-Virus;
- segnalare immediatamente all'amministratore di sistema le stazioni che si rivelino, o vengano indicate, come infette, oppure qualsiasi sospetta presenza di virus che pregiudichi o abbia pregiudicato il sistema, interrompendo qualsiasi attività.
- Porre la massima attenzione nel ricevere, per necessità di svolgimento della propria attività lavorativa, contenuti dalla rete Internet (es. documenti di testo, tabelle, ecc.) cercando di valutare l'attendibilità

del sito a cui si è collegati (ad es. valutando all'interno dell'URL la presenza di estensioni a dominio di dubbia liceità e/o utilizzo dell'indirizzo IP al posto del nome di dominio).

- Nell'utilizzo della posta elettronica:
  - ✓ evitare di aprire allegati che contengono un'estensione doppia o con estensione JS, VBS, SHS, PIF, EXE, COM o BAT;
  - ✓ se si ricevono e-mail non richieste o con contenuti pubblicitari, evitare di seguire i collegamenti a indirizzi Web eventualmente presenti nel testo delle e-mail;
  - ✓ nel caso si riceva un messaggio di e-mail da una persona conosciuta, ma con un contenuto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato; infatti, alcuni virus sono in grado di trasmettere messaggi con allegati che sembrano spediti da mittenti conosciuti;
  - ✓ evitare di cliccare su icone dall'apparenza innocua che ricordano applicazioni associate ad immagini o musica, mostrate dagli allegati di posta elettronica in quanto possono nascondere "worm".

4.7 CARTELLE DI RETE CONDIVISE

Le cartelle di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file personale o che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

All'interno di tali cartelle devono essere identificate dei folder, chiaramente riconducibili all'utente, che devono essere da lui utilizzate come repository del backup dei dati eventualmente conservati nella postazione di lavoro assegnata o come locazione per la conservazione dei documenti trattati nel proprio lavoro.

Particolare attenzione deve essere prestata alla duplicazione dei dati sulle unità di rete. È assolutamente da evitare un'archiviazione ridondante.

4.8 UTILIZZO DELLE STAMPANTI

È cura dell'utente effettuare la stampa dei dati solo se questa è strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni in quanto è buona regola non dimenticare documenti nelle stampanti, fotocopiatrici o fax.

In caso di stampa di documento nelle stampanti poste in aree comuni il titolare della stampa dovrà:

- ✓ recarsi immediatamente presso la postazione oggetto della richiesta di stampa;
- ✓ attendere il completamento dell'operazione di stampa e ritirare tutti i fogli generati;
- ✓ distruggere immediatamente i fogli stampati erroneamente;
- ✓ contattare immediatamente l'amministratore di sistema oppure il tecnico addetto alle stampanti, segnalando eventuali blocchi o anomalie riscontrate in fase di stampa, laddove questi manifestino una particolare gravità.

4.9 UTILIZZO DI INTERNET

Il libero accesso alla rete Internet espone il Liceo Giorgione ed i dipendenti a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge 22 aprile 1941 n. 633 sul diritto d'autore e normativa sulla privacy Reg. UE 2016/679, fra tutte), creando evidenti problemi alla sicurezza. Pertanto, si precisa quanto segue:

4.9.1 Principi generali

Per il personale dell'Istituto, il pc costituisce uno **strumento di lavoro**, necessario allo svolgimento della propria attività lavorativa. È quindi da ritenersi PROIBITA la navigazione in Internet attraverso il personal computer in dotazione per motivi diversi da quelli strettamente concernenti lo svolgimento dell'attività lavorativa stessa.

È inoltre fatto divieto all'utente, lo scarico e l'installazione di software prelevato da siti Internet o da altre fonti, così come ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
Inoltre, è vietata, salvo specifica ed esplicita autorizzazione del Dirigente scolastico:

- la partecipazione a forum non professionali;
- l'utilizzo di chat (esclusi gli strumenti espressamente autorizzati);
- l'utilizzo di bacheche elettroniche;
- le registrazioni in guest books anche utilizzando pseudonimi (o nicknames);
- l'utilizzo di social networks.

4.9.2 Configurazione di sistemi e l'utilizzo di filtri che prevengano determinate operazioni

La navigazione Internet per gli utenti della rete scolastica è regolamentata in modo da tutelare il Liceo Giorgione nell'ambito della vigente normativa attraverso un sistema di Web Filtering che consente la definizione e l'applicazione di policy sull'utilizzo di Internet.
Il sistema di Web Filtering offre una funzionalità di filtraggio Internet accurata in grado di bloccare spyware e altre minacce via web compresi virus, cavalli di Troia, worm, keylogging, phishing, etc.
Ai fini del controllo della regolarità del traffico internet e dell'efficienza della banda utilizzata, la navigazione Internet può essere sottoposta a monitoraggio e registrazione. In queste attività di monitoraggio e registrazione, a tutela dei dati personali, i nomi degli utenti sono anonimizzati automaticamente dal sistema; qualora ne sussistessero le condizioni legittime e solo con l'autenticazione tramite opportune credenziali è possibile togliere l'anonimato per risalire all'utente che abbia compiuto una violazione. I log di navigazione vengono conservati per 30 giorni.

4.10 POSTA ELETTRONICA

Sebbene le caselle di posta elettronica siano assegnate alla "funzione" e non ai singoli utenti, si rammenta che queste sono **strumenti di lavoro,** che rimangono di esclusiva proprietà del Liceo Giorgione, anche dopo la cessazione del rapporto lavorativo; pertanto, le persone che hanno l'accesso a tali caselle di posta sono direttamente responsabili del corretto utilizzo e funzionamento, e devono mantenerla in ordine.
Queste le regole comportamentali da tenere:

- la posta elettronica non va utilizzata ai fini personali, ma unicamente a fini lavorativi e in questo senso l'assegnatario della casella di posta elettronica ne autorizza sin da ora la consultazione da parte di soggetti espressamente autorizzati dal Liceo Giorgione, nell'ambito dei controlli da questo effettuati. La posta elettronica non va utilizzata come strumento di archiviazione dati, che viene assicurata attraverso altri canali, quali ad esempio lo spazio messo a disposizione nelle unità di rete. In ogni caso l'assegnatario della casella di posta elettronica, salvo il caso fortuito o evento tecnico a lui non imputabile, si impegna a preservare il contenuto delle e-mail comprensivo di tutti i dati;
- la lista dei destinatari della corrispondenza elettronica deve essere strettamente limitata alle persone che hanno effettiva necessità di essere messe a conoscenza del contenuto del messaggio stesso:
  - ✓ il destinatario di una comunicazione A: (per competenza) è colui al quale deve giungere in quanto ci si aspetta che faccia e/o decida qualcosa
  - ✓ il destinatario di una comunicazione CC: (per conoscenza) è colui il quale deve semplicemente conoscere la comunicazione senza fare e/o decidere alcunché;
- il comando "rispondi a tutti" deve essere utilizzato solo nel caso tutti i destinatari (compresi i destinatari "per conoscenza") abbiano effettiva necessità di essere informati della risposta;
- la comunicazione di lavoro inquadrata all'interno di un'organizzazione deve rispondere a requisiti di efficienza e di pertinenza e, in termini generali, deve pertanto essere inviata solamente alla persona

titolata a gestire l'informazione. Non effettuare pertanto escalation verso i responsabili della persona destinataria se non in caso di mancata risposta in tempi ragionevoli, meglio se indicati nel contenuto del messaggio originale;

- è vietato l'utilizzo della posta per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione o necessità legate alle attività lavorative opportunamente giustificate;
- sono da evitare messaggi estranei al rapporto di lavoro o alle relazioni tra colleghi;
- è obbligatorio controllare i file allegati ai messaggi di posta elettronica prima del loro utilizzo (non eseguire il download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

4.11 REGISTRO ELETTRONICO DI CLASSE E DEL DOCENTE

Tutti i docenti sono tenuti ad apporre firma elettronica per le proprie ore di lezione, annotare gli argomenti oggetto della lezione, segnalare e giustificare le assenze, i ritardi e le uscite anticipate, scrivere gli avvisi per le famiglie, eventuali note disciplinari o annotazioni personali. In particolare, è affidato al docente della prima ora il compito di segnare o giustificare le assenze degli alunni.
Se, per qualunque ragione, non fosse possibile utilizzare il registro elettronico, il docente dovrà prendere nota delle informazioni e/o dei dati da inserire nel registro e appena possibile li inserirà in quest'ultimo.
I voti delle discipline riportano la data di svolgimento della prova ed eventuali annotazioni per la famiglia e sono consultabili dal Docente che li ha assegnati, dal Coordinatore di classe, dal Dirigente Scolastico e dai genitori dello studente.

4.12 COMUNICAZIONI SCUOLA-FAMIGLIA

I genitori, per avere accesso al registro elettronico, devono compilare e firmare un apposito modulo e ricevere dalla segreteria della scuola le credenziali di accesso: username e password.
Il software in uso (Infoschool) consente anche di programmare i colloqui con le famiglie: ogni docente scriverà a inizio anno i giorni e l'orario di ricevimento e stabilirà quanti genitori possono iscriversi ogni volta e con quanti giorni di preavviso. Al momento della conferma, il programma assegnerà al genitore un numero progressivo di prenotazione.
Rimane naturalmente la libertà del docente di concordare tempi e modi per altre occasioni di confronto con le famiglie per situazioni particolari che lo richiedono.

4.13 UTILIZZO DELLA RETE INFORMATICA

La rete wi-fi o cablata dell'Istituto deve essere utilizzata con prudenza e diligenza.
È vietato scaricare software, musica, filmati, immagini illegali o vietati ai minori.
Ogni utente è responsabile dell'utilizzo della rete e si impegna a mantenere segrete e a non comunicare a terzi la password d'ingresso della rete e ai programmi e a non permettere ad alcuno di utilizzare il proprio accesso.
Infine, occorre preventivamente scansionare con antivirus ogni archivio elettronico (file) acquisito attraverso qualsiasi supporto (es. pen drive) prima di trasferirlo su aree comuni della rete.
Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività della rete, interferire con la connettività altrui o con il funzionamento del sistema e quindi di:

- utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti, utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
- sostituirsi a qualcuno nell'uso di sistemi, cercare di catturare password altrui o forzare password o comunicazioni criptate;
- modificare le configurazioni imposte dall'Amministratore di Sistema;
- limitare o negare l'acceso al sistema a utenti legittimi;
- distruggere o alterare dati altrui;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

5 RICHIESTA DI ASSISTENZA

Per quanto concerne le richieste di assistenza IT, siano esse relative a qualsiasi problematica inerente alle postazioni di lavoro, ai dispositivi in genere (stampanti, scanner ecc.) e/o alle applicazioni e/o generici dubbi su quale comportamento adottare, la procedura prevede l'inoltro di una e-mail agli assistenti tecnici informatici oppure all'amministratore di sistema all'indirizzo: …… (inserire indirizzo amministratore di sistema e nucleo informatico)

Per richieste di assistenza relative a sblocco account o reset della password possono essere richieste solo dal titolare delle credenziali.

6 CONTROLLI

Controlli periodici e/o occasionali per ragioni legittime, specifiche e non generiche, verranno effettuati esclusivamente da soggetti autorizzati dal Dirigente scolastico.

Tali ragioni legittime possono essere:

- verifica del corretto utilizzo degli strumenti di lavoro (es. pc);
- evitare la perpetrazione di comportamenti illeciti e/o abusi informatici;
- blocco del PC, infezione da virus non rilevato dal sistema di sicurezza;
- guasto di elementi hardware che rendono impossibile la prosecuzione dall'attività lavorativa;
- instabilità o blocco di sistemi software o della Linea Internet.

Graduazione dei controlli

I controlli iniziali, riferibili a navigazioni non autorizzate, saranno riferiti alla totalità degli utenti. Il perdurare delle attività di navigazione non consentite autorizzano il Liceo Giorgione a scendere ulteriormente nel particolare, effettuando controlli al livello di gruppi omogenei. In caso di extrema ratio, qualora si rilevino ulteriori abusi che possano precludere la sicurezza dei sistemi informativi, possano essere lesivi del patrimonio scolastico e possano identificare anche reati di natura penale, l'attività di controllo verrà effettuata con modalità di identificazione personale.

Verifica sui dati aggregati per area

↓

Avviso generalizzato a rispettare le istruzioni e compiti

↓

Controlli individuali

Modalità di controllo

I controlli verranno svolti nel rispetto della libertà e dignità dei prestatori di lavoro, nonché nel rispetto dei principi di correttezza, pertinenza e non eccedenza.

Coloro che dovessero violare quanto disposto dal presente regolamento saranno soggetti alle azioni disciplinari ai sensi del D.lgs. 150/2009 e del D.lgs. 165/2001.

7 SOGGETTI PREPOSTI

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, sarà posta opportuna cura nella prevenzione di accessi illegittimi a dati personali presenti in cartelle o spazi di memoria.

I soggetti preposti al trattamento dei dati (in particolare, gli incaricati della manutenzione) svolgeranno solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

I soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi sono edotti e consapevoli delle linee di condotta da tenere, attraverso un'adeguata attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

8 ISTRUZIONI IMPARTITE DAL TITOLARE

Le presenti indicazioni operative sono rivolte a tutti gli incaricati del trattamento dei dati.

1) L'incaricato del trattamento dovrà aver accesso ai soli dati personali la cui conoscenza è strettamente necessaria per adempiere ai compiti a lui assegnati.
2) L'incaricato dovrà controllare e custodire gli atti e i documenti contenti i dati personali per l'intero ciclo necessario allo svolgimento delle operazioni.
3) All'incaricato compete la conservazione degli atti e dei documenti a lui affidati; l'incaricato stesso provvederà a restituirli al termine delle operazioni affidate.
4) L'incaricato, in caso di trattamento di dati sensibili o di dati giudiziari, dovrà controllare e custodire gli atti e i documenti a lui affidati, fino alla restituzione, in maniera che a essi non accedano persone prive di autorizzazione, e restituirli al termine delle operazioni affidate.
5) L'incaricato dovrà conservare e custodire i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento dei dati sensibili o dati giudiziari osservando le misure sopradescritte.
6) L'incaricato, nelle operazioni di trattamento, dovrà ridurre al minimo i rischi di distruzione e perdita.
7) L'incaricato che effettua operazioni di trattamento mediante l'ausilio di strumenti elettronici o automatizzati dovrà utilizzare il codice identificativo e la parola chiave a lui forniti dal Titolare, attraverso l'Amministratore di Sistema, e custodirli con la dovuta riservatezza.
8) L'incaricato dovrà modificare la parola chiave al primo utilizzo e alle scadenze previste, ogni 90 giorni, secondo le istruzioni fornite dall'amministratore di sistema.
9) L'incaricato non dovrà lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento (seguendo le istruzioni operative impartite dall'Amministratore di Sistema o dagli incaricati alla manutenzione e gestione degli strumenti elettronici)
10) Nel caso di utilizzo di supporti di memorizzazione contenenti dati sensibili o dati giudiziari, l'incaricato potrà riutilizzarli qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti dovranno essere distrutti.

9 CONCLUSIONI

Il presente regolamento, condiviso nel Collegio Docenti del_____, approvato dal Consiglio d'Istituto con delibera n._____ del_____, costituisce parte integrante del Regolamento di Istituto e viene affisso all'Albo on-line della Scuola, per garantire la massima visibilità da parte di tutti.