

## **Norme generali**

- 1 Il dirigente scolastico (DS) individua l'amministratore di rete e i responsabili dei vari laboratori di informatica. Tali figure rimangono in carica per un anno scolastico e comunque fino a nuova nomina, di norma entro il mese di settembre.
- 2 Ogni utilizzatore delle strutture informatiche, consapevole delle potenzialità offerte dagli strumenti informatici e telematici, si impegna a non commettere abusi aderendo ad un principio di autodisciplina fondato sul presente regolamento
- 3 Ogni utilizzatore delle strutture informatiche dovrà essere adeguatamente formato in merito alle problematiche relative alla sicurezza nei laboratori e alle norme elementari relative all'uso dei dispositivi elettronici, ivi comprese le buone pratiche di ergonomia.
- 4 Il docente in aula, eventualmente coadiuvato dall'insegnante tecnico pratico e dall'assistente tecnici di laboratorio, è tenuto a vigilare sull'utilizzo delle strutture informatiche e dei dispositivi da parte degli studenti e all'applicazione del presente regolamento.
- 5 L'utente che ottiene l'accesso alla rete (docente o studente) si assume la totale responsabilità delle attività svolte tramite la stessa; è pertanto necessario porre attenzione all'utilizzo delle strutture, alla conservazione proprie password e all'applicazione del presente regolamento.
- 6 Qualsiasi accesso alla rete viene monitorato ed è associato ad una persona fisica cui imputare le attività svolte utilizzando il codice utente, la password, l'identificatore unico di macchina. Di tutte le attività svolte resta una traccia che viene debitamente conservata in ottemperamento alle norme vigenti e nel rispetto della normativa sulla privacy.
- 7 L'accesso ad alcuni servizi è consentito all'utente mediante l'utilizzo delle credenziali per l'accesso alla rete scolastica e al registro elettronico o ad altri portali scolastici. Tali credenziali, contenendo informazioni identificative, sono strettamente personali e pertanto non cedibili. Qualora dovessero essere cedute ad altri, la responsabilità delle attività da costoro svolte in rete ricadrà in ogni caso sul titolare delle credenziali. È quindi responsabilità dell'utente la custodia dei propri codici di accesso ai servizi. Qualora l'utente avesse il sospetto che le proprie credenziali siano state violate, avrà il dovere di procedere tempestivamente alla modifica della password e segnalare l'accaduto al DS. È bene tenere presente che né l'istituto né i fornitori di cui questo si avvale richiederanno mai la trasmissione delle credenziali via mail
- 8 È vietato intraprendere scansioni della rete e/o attacchi alla sicurezza informatica. L'infrastruttura di rete è dotata di strumenti automatici per il rilevamento di attacchi e l'individuazione di utenti e terminali da cui questi provengono. È fatto divieto di distribuire in rete materiali o strumenti che violino la legge sul diritto d'autore e sulla proprietà intellettuale. Non è consentito usare in nessun caso la rete di Istituto (wireless o cablata) per scambiare materiale illegale: lo scambio di materiale protetto da copyright (MP3, film, software commerciale, ecc...) è vietato per legge e soggetto a sanzioni penali. In caso di rilevamento di azioni illegali l'Istituto prenderà i provvedimenti previsti e metterà a disposizione delle autorità che ne facessero richiesta tutta la relativa documentazione.
- 9 È vietato utilizzare la rete di istituto per l'invio di messaggi pubblicitari/promozionali o immettere in rete comunicazioni/informazioni che possano presentare forme o contenuti di carattere razzista, pornografico, osceno, blasfemo, diffamatorio ed offensivo.
- 10 L'uso della fotocamera e dei registratori audio e video in istituto (sia nei momenti formali che informali) è vietato. Agli studenti è consentito solo se autorizzato dall'insegnante e solo per uso strettamente personale, funzionale all'apprendimento. In caso di violazione della norma si procederà al ritiro del terminale che verrà riconsegnato ai genitori. Non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. La

diffusione di materiali che ledono la riservatezza e la dignità delle persone può far incorrere l'utente in sanzioni disciplinari ed anche in veri e propri reati come previsto dalle norme vigenti in materia. Nel caso il materiale diffuso leda la riservatezza e la dignità delle persone (docenti, studenti, visitatori), il dirigente scolastico segnalerà tali violazioni agli organi di polizia competenti, oltre agli eventuali provvedimenti disciplinari.

11 È vietato far utilizzare ad altri utenti, anche compagni di classe, il proprio terminale. Ogni utente può utilizzare unicamente ed esclusivamente il proprio terminale. L'utente che farà utilizzare il proprio terminale ad altri utenti sarà responsabile dei danni eventualmente causati da questi e verrà sottoposto alle norme disciplinari previste. Per tali motivi l'utente non potrà mai abbandonare il proprio terminale, né darlo in custodia ad altro utente.

12 Il personale che opera con la rete deve provvedere ad effettuare copie di backup del lavoro svolto. Tali supporti dovranno essere custoditi in luogo sicuro.

13 Gli allievi, gli esterni e il personale non preposto non possono e non devono accedere, né fisicamente né digitalmente, ai siti in cui sono custoditi dati e/o informazioni sensibili.

14 Il calendario delle lezioni con utilizzo dei laboratori e delle postazioni di informatica deve essere stabilito dagli incaricati della stesura dell'orario all'inizio di ogni anno scolastico in coordinamento con l'ufficio tecnico e il dirigente.

15 L'accesso ai laboratori e/o alle postazioni di informatica in momenti extrascolastici deve essere autorizzato e concordato con l'ufficio tecnico. I collaboratori scolastici riceveranno il calendario con le autorizzazioni.

16 I docenti che accompagnano gruppi di allievi devono stabilire per ognuno di loro la postazione che occuperà per tutto l'anno scolastico; i docenti compileranno lo schema piantina e consegneranno copia al responsabile del laboratorio. Copia di tutti gli schemi di assegnazione postazioni sarà consegnato a cura del Responsabile di Laboratorio all'ufficio tecnico.

17 All'ingresso in laboratorio si deve accertare che tutto sia in ordine. Ove si riscontrassero malfunzionamenti o mancanze ci si dovrà riferire prontamente, senza manipolare alcunché, al responsabile del laboratorio o al DS.

18 Nei laboratori gli allievi dovranno compilare il modulo di postazione sul quale anoteranno data, orario di utilizzo, classe e nominativi.

19 La richiesta e il conseguente spostamento di apparecchiature multimediali in altro laboratorio o in aula, se non previsto nel piano orario di utilizzo, deve essere richiesto con congruo anticipo al Responsabile di Laboratorio.

20 Gli allievi devono sistemare gli zaini in una zona del laboratorio che non impedisca un regolare sfollamento, non si arrechi danno agli impianti, non risulti in violazione alle norme della sicurezza.

21 Non è possibile cambiare di posto le tastiere, le stampanti, i mouse, le casse o qualunque altra attrezzatura senza autorizzazione del Responsabile di Laboratorio.

22 Il personale e gli allievi dovranno aver cura di rispettare le procedure corrette di accensione, di utilizzo e di spegnimento delle macchine, è vietato in ogni modo accedere agli impianti sia elettrici sia telematici. È vietato mangiare o ingerire liquidi nei laboratori.

23 È possibile l'utilizzo di chiavette personali solo previa autorizzazione del responsabile di laboratorio e sotto la diretta sorveglianza del docente o del responsabile di laboratorio.

24 L'uso delle stampanti avviene solo a conclusione del lavoro ed è subordinato a una preventiva antepresa di stampa per evitare spreco di carta e di inchiostro.

25 Qualora l'utente rilevi malfunzionamenti o riceva messaggi ignoti dal sistema o dall'antivirus

installato sul proprio PC deve cessare immediatamente ogni attività e rivolgersi prontamente al docente in aula o al responsabile di laboratorio.

26 Prima di uscire dal laboratorio occorre accertarsi che le sedie siano al loro posto, che non vi siano cartacce o rifiuti e che tutte le apparecchiature siano spente correttamente.

27 In ogni ambiente è conservata la manualistica del software e dell'hardware delle postazioni presenti. Per accedere alla manualistica occorrerà riferirsi al responsabile di laboratorio.

28 Per motivi di manutenzione ordinaria e/o straordinaria, i PC possono essere riformattati dai responsabili senza alcun preavviso. Si consiglia pertanto di salvare i dati nei supporti di memoria in dotazione.

29 Periodicamente il responsabile di laboratorio provvederà a coordinare l'aggiornamento del software di sistema e dei vari applicativi in uso.

30 Le password delle postazioni in laboratorio sono note solo al responsabile di rete e agli assistenti tecnici di ciascun laboratorio, che sono gli unici autorizzati a intervenire per la manutenzione e l'aggiornamento delle macchine. Una copia aggiornata delle credenziali è consegnata al DS.