



ISTITUTO TECNICO “CAMILLO MORIGIA - LUIGI PERDISA”

Sede amministrativa, indirizzi **Geometri e Grafica**:
Via Guglielmo Marconi 6 – 48124 Ravenna,
☎ 0544-400287; Fax: 0544-400289

Sede indirizzo **Agrario e Azienda Agraria**:
Via Dell'Agricoltura 5 – 48123 Ravenna;
☎ 0544-450079; Fax: 0544-450787

E-Mail: ratl02000l@istruzione.it
PEC: ratl02000l@pec.istruzione.it
WEB: <http://www.itmorigiaperdisa.it>
Codice Fiscale n. 92082620391

REGOLAMENTO DI ACCESSO AL NETWORK DI ISTITUTO E NORME DI COMPORTAMENTO.

- a) Tutti i docenti e il personale A.T.A. dell'Istituto hanno diritto ad un account per l'uso delle postazioni informatiche collocate nei Laboratori Didattici od in altri luoghi con collegamento alla rete cablata o WiFi. Gli account sono riservati ad un uso didattico o di servizio, sono strettamente personali e non cedibili. Si declina ogni responsabilità per un uso diverso da quello didattico.
- b) Gli studenti potranno essere dotati di un account/password per l'accesso alle risorse informatiche di Istituto ed alla Google Suite (ex Google Apps for Education) ma non sarà disponibile un accesso personale alla rete interna tramite WiFi per cui si rimanda alla rete pubblica WISPER.
- c) Validità e utilizzo degli account: Gli account di posta elettronica degli studenti sono aperti al solo dominio @itmorigiaperdisa.it; per uso didattico, alcuni domini esterni, potranno essere abilitati alla ricezione della posta.
- d) Gli account degli studenti rimarranno attivi fino al conseguimento del diploma o finché non avvenga un trasferimento ad altro istituto; terminato il rapporto formativo con l'istituto “Morigia-Perdisa” l'account viene sospeso salvo situazioni particolari che saranno valutate su richiesta. Dopo 30 giorni dalla terminazione del rapporto con l'Istituto l'account, sempre salvo situazioni particolari, può essere cancellato definitivamente e senza preavviso.
- e) Gli account del personale interno rimarranno attivi fino a 40 gg. dal trasferimento ad altra scuola o cessazione del rapporto di lavoro; oltre questo termine, l'account del personale viene sospeso. Per questo motivo si raccomanda di non utilizzare l'account username@itmorigiaperdisa.it per gestire e archiviare comunicazioni e documenti strettamente personali.
- f) La piattaforma è concessa in uso gratuito al personale in servizio e agli studenti per lo svolgimento delle attività didattiche e dei progetti d'istituto. Dopo 2 anni dalla sospensione dell'account tutti i dati e i file ancora presenti nella home directory e nel cloud drive dell'utente potranno essere cancellati dall'amministratore senza preavviso. I file presenti nelle singole postazioni di lavoro dei laboratori potranno essere invece spostati/cancellati in caso di

riorganizzazione e o ripristino della postazione in qualsiasi momento e senza preavviso. Le postazioni di lavoro dedicate al personale della segreteria e/o tecnico sono in uso al solo a detto personale, l'utilizzo e il backup delle informazioni ivi memorizzate è di responsabilità di detto personale.

- g) Gli account vengono assegnati dall'Amministratore di sistema/rete o da una persona espressamente delegata da quest'ultimo, dietro richiesta scritta. L'ottenimento di un account comporta l'impegno a rispettare, oltre alle norme di legge vigenti in materia di sicurezza informatica, protezione del copyright e della privacy, il presente regolamento e sue eventuali modifiche in seguito pubblicate, nonché i regolamenti delle reti esterne (Internet ecc..) e dei nodi cui eventualmente ci si connetta. Informazioni e chiarimenti tecnici sul funzionamento della rete locale potranno essere richiesti all'Amministratore di sistema o all'Amministratore di rete.
- h) Il titolare di un account (da ora in poi definito genericamente utente) sarà ritenuto responsabile di tutte le operazioni eseguite durante la sessione attivata con l'account stesso. Le password devono essere sequenze non banali di almeno otto simboli. Parole di senso compiuto, date, parti di codice fiscale, acronimi e anagrammi e simili sono password banali. Le password dovranno contenere, preferibilmente, non solo caratteri alfabetici ma anche numerici e simboli speciali. Ogni utente si impegna a cambiare la propria password al più ogni sei mesi e comunque quando ciò venga richiesto dagli amministratori del sistema o automaticamente dal sistema operativo di rete. La nuova password, in ogni caso, dovrà essere sempre non banale e indipendente dalla precedente, non una variazione di quest'ultima. Gli utenti sono quindi invitati a conservare con cura la propria password, a non cederla a terzi e a non lasciare sessioni incustodite. L'entrata e l'uscita da ogni laboratorio didattico deve essere anche annotata in un apposito "registro" cartaceo o informatico.
- i) L'uso delle risorse non deve mettere a rischio la sicurezza dei Laboratori didattici o di altro sistema.
- j) L'uso delle risorse del sistema da parte di ogni utente non dovrà provocare un rallentamento continuativo e prolungato del sistema o avere gravi riflessi negativi sull'attività lavorativa altrui. Ogni utente è tenuto a rispettare le quote di risorse assegnate ove queste siano stabilite (e.g. occupazione spazio-disco) e a non danneggiare gli altri utenti abusando delle risorse comuni (per esempio stampanti).
- k) È fatto divieto, quando non espressamente previsto, di copiare il software in uso al dipartimento sottoposto a licenza d'uso commerciale di cui l'Istituto ne sia licenziatario e destinarlo ad usi diversi da quelli per cui è stato acquistato. Ogni utente è responsabile dei

dati e dei programmi presenti nelle proprie aree di lavoro. La licenza d'uso del software presente nella propria cartella personale (home directory) deve autorizzare l'utente in modo regolare. Possono essere pubblicate sulla rete locale, dall'amministratore di sistema o suo delegato, cartelle "repository" per software da installare, sia didattico che operativo, al fine di migliorare la fruibilità delle risorse informatiche disponibili nell'Istituto.

- l) Ogni utente ha la facoltà di utilizzare dal proprio account tutti i servizi di rete resi disponibili; a tale scopo possono essere forniti, se tecnicamente possibile e su richiesta scritta al Dirigente Scolastico, un account di e-mail, e un account per la pubblicazione di materiale sul sito Web dell'Istituto. Ogni utente è personalmente responsabile di ciò che pubblica e spedisce. È fatto divieto di esprimere posizioni ufficiali dell'Istituto o prendere impegni in nome dell'Istituto se non preventivamente autorizzati dal dirigente competente.
- m) Eventuali deroghe al presente regolamento legate a particolari esigenze devono essere autorizzate in forma scritta dal Dirigente Scolastico dell'Istituto.
- n) Gravi violazioni al presente regolamento o alle norme di Legge in materia comporterà una segnalazione ufficiale al Dirigente Scolastico, che provvederà a far sospendere l'account per un periodo dipendente dalla gravità dell'infrazione. Naturalmente poiché la responsabilità per infrazioni di rilevanza civile o penale resta personale, oltre ai provvedimenti disciplinari citati l'utente può incorrere nelle sanzioni previste dalla Legge.
- o) È vietato l'uso di applicazioni che possono saturare la banda disponibile per le comunicazioni impedendo ad altri utenti l'uso della rete. L'uso di tali programmi può essere consentito, previa autorizzazione al Dirigente Scolastico o suo delegato per periodi limitati e solo per scopi didattici o di servizio.
- p) L'accesso ad Internet da parte degli studenti per mezzo della rete cablata deve essere esplicitamente richiesto e autorizzato dal personale Docente responsabile della classe e/o all'Assistente Tecnico. Essi utilizzeranno l'account della propria classe sotto sorveglianza del Docente presente in aula che se ne assume, perciò, la responsabilità.
- q) È vietato consultare servizi Internet per scopi non didattici o non di servizio e utilizzare materiale in violazione del diritto d'autore e di copyright. È vietato consultare materiale offensivo, di fanatismo, razzismo, pornografico, gioco d'azzardo o di quanto altro possa risultare non legato a scopi didattici o di servizio. Qualora, inavvertitamente, si abbia accesso a tale materiale si deve informare tempestivamente l'Amministratore di sistema (che ha l'accesso al firewall) o all'Amministratore di rete che provvederà ad aggiornare, per quanto tecnicamente possibile, i filtri di navigazione.

- r) Ogni persona è totalmente responsabile delle proprie credenziali d'accesso che sono personali e non cedibili (riferimento legge 23 dicembre 1993 n. 547 e successive modifiche). Gli accessi alla rete sono registrati nei "log".
- s) L'amministratore di sistema e/o l'amministratore di rete, su delega del Dirigente Scolastico, hanno facoltà di modificare il funzionamento tecnico dei sistemi operativi e degli apparati di rete locale per apportare, dove tecnicamente possibile, correzioni migliorative o funzionali, nel rispetto di quanto riportato all'allegato B del **Decreto legislativo 30 giugno 2003, n. 196**.
- t) Per motivazioni di carattere tecnico, d'opportunità, o per l'insorgere di situazioni non contemplate nel presente Regolamento che necessitino di essere disciplinate, potranno essere proposte modifiche e/o integrazioni al presente Regolamento, che saranno tempestivamente comunicate.
- u) Norma transitoria: la richiesta scritta per l'ottenimento di "account utente" e di impegno al rispetto del regolamento della rete deve essere formalizzata anche dagli utenti con account già attivo. In caso di mancata formalizzazione, dopo la consegna delle credenziali, l'account potrà essere sospeso dall'amministratore di rete.
- v) La nomina degli amministratori di rete e dei sistemi server, degli amministratori dei sistemi client, e degli amministratori delle Basi di Dati per il trattamento dei dati personali, è effettuata dal Dirigente Scolastico o delegato, dal Direttore Generale dei Servizi Amministrativi o delegato.

NORME DEL CODICE PENALE IN TEMA DI CRIMINALITÀ INFORMATICA

Legge 23 dicembre 1993 n. 547 Art. 420 (attentato a impianti di pubblica utilità)

Chiunque commette un fatto diretto a danneggiare impianti di pubblica utilità è punito, salvo che il fatto costituisca più grave reato, con reclusione da 1 a 4 anni. (...) se dal fatto deriva la distruzione delle informazioni o dei dati o dei programmi, ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema la pena è della reclusione da 3 a 8 anni.

Art. 615-ter (Accesso abusivo ad un sistema informatico o telematico)

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo è punito con la reclusione fino a 3 anni. Se dal fatto deriva il danneggiamento del sistema, la distruzione di dati o l'interruzione del servizio la pena è la reclusione da 1 a 5 anni. Nel caso la violazione riguardi sistemi informatici di interesse militare, ordine pubblico, sicurezza pubblica, sanità, protezione civile o comunque di interesse pubblico la pena è rispettivamente da 1 a 5 anni e da 3 a 8 anni.

Art. 615-quater (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici)

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, password o altri mezzi idonei, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad 1 anno e con la multa sino a lire 10 milioni. La pena è della reclusione da 1 a 2 anni e della multa da 10 a 20 milioni se il danno è arrecato ad un sistema informatico di pubblica utilità.

Art. 615-quinquies (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico)

Chiunque diffonda, comunichi o consegna un programma informatico da lui stesso o da altri redatto, avente scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti (...) è punito con la reclusione sino a 2 anni e con la multa sino a lire 20 milioni.

Art. 617-quater (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche)

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico ovvero le impedisce o le interrompe è punito con la reclusione da 6 mesi a 4 anni: La reclusione è da 1 a 5 anni se il fatto è commesso in danno di un sistema informatico di pubblico interesse.

Art. 617-quinquies (Installazione di apparecchiature atte ad intercettare, impedire o di interrompere comunicazioni informatiche)

Chiunque, salvo i casi consentiti dalla legge, installa apparecchiature ovvero programmi, atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico è punito con la reclusione da 1 a 4 anni: Nel caso di sistemi informatici di pubblico interesse la pena è aumentata da 1 a 5 anni.

Art. 635-bis (Danneggiamento di sistemi informatici o telematici)

Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da 6 mesi a 3 anni.

Art. 640-ter (Frode informatica)

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o intervenendo senza diritto su dati, informazioni o programmi contenuti in un sistema informatico, procura a sé o a terzi un ingiusto profitto con altrui danno, è punito con la reclusione da 6 mesi a 3 anni e con la multa fino a 2 milioni.