ISTITUTO COMPRENSIVO N.1 - PORTO TORRES
SCUOLA DELL'INFANZIA - SCUOLA PRIMARIA – SCUOLA SECONDARIA 1° GRADO
Tel. 079/5048912 - Fax 079/501001 - e-mail: ssic841007@istruzione.it PEC: ssic841007@pec.istruzione.it
www.comprensivo1portotorres.gov.it

A tutto il Personale Docente e ATA
Al DSGA
Al Sito Istituzionale

REGOLAMENTO PER L'UTILIZZO DELLA RETE INFORMATICA

ART. 1 OGGETTO E AMBITO DI APPLICAZIONE

- Il presente regolamento disciplina le modalità di accesso, di uso della rete informatica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire all'interno e all'esterno dell'Istituzione scolastica.
- La rete dell'Istituzione scolastica dell'Istituto Comprensivo n. 1 di Porto Torres è costituita dall'insieme delle risorse informatiche, cioè dalle risorse infrastrutturali e dal patrimonio informativo digitale.
- Le risorse infrastrutturali sono le componenti *hardware*/*software* e gli apparati elettronici collegati alla rete informatica della scuola. Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.
- Il presente regolamento si applica a tutti gli utenti interni ed esterni che sono autorizzati ad accedere alla rete della scuola. Per utenti interni si intendono tutti gli amministrativi, i docenti e i collaboratori scolastici. Per utenti esterni si intendono le ditte fornitrici di *software* che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, enti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle stesse e i collaboratori esterni.

ART. 2 PRINCIPI GENERALI – DIRITTI E RESPONSABILITÀ

- L'Istituto Comprensivo n. 1 di Porto Torres promuove l'utilizzo della rete informatica, di internet e della posta elettronica quali strumenti utili a perseguire le proprie finalità istituzionali.
- Ogni utente è responsabile **civilmente** e **penalmente** del corretto uso delle risorse informatiche, dei servizi/programmi ai quali ha accesso e dei propri dati.
- Il presente regolamento considera i divieti posti dallo Statuto dei Lavoratori sul controllo a distanza (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 legge 20 maggio 1970, n. 300), rispettando durante i trattamenti i principi di necessità (art. 3 del Codice; par. 5.2), correttezza (art. 11, comma 1, lett. a) e finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b del Codice par. 4 e 5).
- Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella rete informatica è sottoposta a registrazione in appositi *file* e riconducibili ad un *account* di rete. Detti *file* possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo e possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal D.Lgs. n. 196/2003 e normativa collegata.
- A tutela del dipendente, qualora l'Istituto decidesse di perseguire, per fini legati alla sicurezza dell'intero sistema informativo, il controllo della posta e della navigazione in internet, prima di iniziare il trattamento comunicherà gli strumenti e i modi di trattamento effettuati. Tale compito sarà demandato all'Amministratore di Sistema esterno, a garanzia e tutela delle informazioni di carattere personale dei lavoratori.
- L'Amministratore di Sistema cura l'attuazione del presente regolamento attraverso la predisposizione di Procedure Operative che verranno diffuse tra tutti i dipendenti.
- Tali procedure nonché il presente regolamento devono essere rese facilmente e continuativamente disponibili per consultazione sui normali mezzi di comunicazione all'interno della struttura.

ART. 3 UTILIZZO DEI PERSONAL COMPUTER

- Il *personal computer* affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza e pertanto è **vietato**.

In particolare:

a) L'accesso all'elaboratore deve essere protetto da *password* che viene custodita dal Titolare del trattamento dati e non divulgata. La *password* deve essere attivata per l'accesso alla rete, per lo *screensaver* e per il *software* applicativo. Non è consentita l'attivazione della *password* di accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

b) L'Amministratore di Sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, avrà la facoltà di accedere in qualunque momento anche da remoto (dopo aver richiesto l'autorizzazione all'utente interessato) al *personal computer* di ciascuno.

c) Il *PC* deve essere spento ogni sera, o al termine delle lezioni o del servizio, prima di lasciare gli uffici o i laboratori di informatica, o in caso di assenze prolungate dall'ufficio. 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. Deve essere attivato su tutti i *PC* lo *screensaver* e la relativa *password*.

d) L'accesso ai dati e ai programmi da utilizzare per adempimenti amministrativi presenti nei *computer* degli uffici, potrà avvenire quando si rende indispensabile ed indifferibile l'intervento per esclusive necessità di funzionalità operativa degli uffici e di sicurezza del sistema. In caso di prolungata assenza od impedimento dell'incaricato il responsabile dell'amministrazione potrà autorizzare l'utilizzo delle *password*, all'assistente amministrativo che sostituisce il titolare responsabile del settore lavorativo di appartenenza. Si raccomanda la custodia delle copie delle credenziali garantendo la relativa segretezza.

e) È vietato installare autonomamente programmi informatici sui *server* salvo autorizzazione esplicita dell'Amministratore di Sistema, e sui *PC* salvo autorizzazione del Titolare, in quanto sussiste il grave pericolo di portare virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il *software* esistente, può esporre la struttura a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul *software* (D.Lgs. 518/92 sulla tutela giuridica del *software* e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di *software* regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

f) È vietato modificare le caratteristiche impostate sul proprio *PC*, salvo autorizzazione esplicita dell'Amministratore di Sistema o del Dirigente Scolastico.

g) 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 all'Amministratore di Sistema.

h) È vietata l'installazione sul proprio *PC* di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, *modem*, dischi esterni, *i-pod*, telefoni, ecc.), se non con l'autorizzazione espressa dell'Amministratore di Sistema o del Dirigente Scolastico.

i) Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema o il Dirigente Scolastico, nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

ART. 4 UTILIZZO DELLA RETE INFORMATICA

- Le unità di rete sono aree di condivisione di informazioni strettamente professionali sulle quali vengono svolte regolari attività di controllo, amministrazione e *backup* e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque *file* che non sia legato all'attività lavorativa non può essere dislocato in queste unità, nemmeno per brevi periodi.
- Si parte quindi dal presupposto che i *file* relativi alla produttività individuale vengono salvati sul *server* e i limiti di accesso sono regolarizzati da apposite procedure di sicurezza che suddividono gli accessi tra gruppi e utenti.
- L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni *file* o applicazione che riterrà essere pericolosi per la sicurezza o in violazione del presente regolamento sia sui *PC* degli incaricati sia sulle unità di rete.
- Le *password* d'ingresso alla rete ed ai programmi sono segrete e non vanno comunicate a terzi, tranne (in situazioni di urgenza) quando si rende indispensabile ed indifferibile l'intervento per esclusive necessità di funzionalità operativa degli uffici e di sicurezza del sistema. Il responsabile dell'amministrazione potrà autorizzare l'utilizzo momentaneo delle *password*, all'assistente amministrativo che sostituisce il titolare responsabile del settore lavorativo, anche se per breve pe-

riodo e provvedere alla creazione dell'utente nuovo.

- Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei *file* obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
- È compito dell'Amministratore di Sistema provvedere alla creazione e alla manutenzione di aree condivise sul *server* per lo scambio dei dati tra i vari utenti.

- Nell'utilizzo della rete informatica è fatto **divieto** di:

a) utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento.
b) agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
c) effettuare trasferimenti non autorizzati di informazioni (*software*, dati, ecc);
d) installare componenti *hardware* non compatibili con l'attività istituzionale;
e) rimuovere, danneggiare o asportare componenti *hardware*;
f) modificare i collegamenti della strumentazione o effettuarne di nuovi senza il consenso dei responsabili del laboratorio e/o dell'Amministratore del Sistema;
g) utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare *file* e *software* di altri utenti;
h) 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*;
i) usare l'anonimato o servirsi di risorse che consentano di restare anonimi;

ART. 5 UTILIZZO DI INTERNET

- I *PC* abilitati alla navigazione in *Internet* costituiscono uno strumento necessario allo svolgimento dell'attività lavorativa.
- Nell'uso di internet e della posta elettronica **non** sono **consentite** le seguenti attività:

a) l'uso di *internet* per motivi personali;
b) l'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.);
c) lo scaricamento (*download*) o l'inserimento (upload) di *software* e di *file* non necessari all'attività istituzionale;
d) utilizzare programmi per la condivisione e lo scambio di *file* in modalità *peer to peer* (Napster, Emule, Winmx, e-Donkey, ecc.);
e) accedere a flussi in streaming audio/video da *internet* per scopi non istituzionali;
f) un uso che possa in qualche modo recare qualsiasi danno all'Istituto o a terzi.

ART. 6 UTILIZZO DELLA POSTA ELETTRONICA

- La casella di posta, assegnata dall'Istituto, è uno strumento di lavoro e le persone assegnatarie delle caselle di posta elettronica sono responsabili del loro corretto utilizzo.
- È fatto **divieto** di utilizzare le caselle di posta elettronica della struttura per la partecipazione a dibattiti, *forum* o *mailing-list*, salvo diversa ed esplicita autorizzazione, che esulino dagli scopi della scuola.
- È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
- La documentazione elettronica che viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto, non può essere comunicata all'esterno senza preventiva autorizzazione del Responsabile del trattamento.
- Per la trasmissione di *file* all'interno della struttura è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati (ad esempio per dimensioni superiori a 2 MB è preferibile utilizzare le cartelle di rete condivise).
- È obbligatorio controllare i *file attachments* (ALLEGATI) di posta elettronica prima del loro utilizzo (non eseguire *download* di *file* eseguibili o documenti da siti Web, HTTP o FTP non conosciuti) e accertarsi dell'identità del mittente.

- In particolare nell'uso della posta elettronica **non** sono **consentite** le seguenti attività:

a) la trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (D.lgs. 196 del 30/6/2003) e inerenti le ragioni di servizio;
b) l'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente;

c) inviare tramite posta elettronica *user-id*, *password*, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici.

ART. 7 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.
- 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.
- 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.
- 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 (punto 5 del disciplinare tecnico).
- 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.
- Qualora l'utente venisse a conoscenza delle *password* di altro utente, è tenuto a darne immediata notizia, per iscritto, al Titolare.

ART. 8 UTILIZZO DEI SUPPORTI MAGNETICI

- Tutti i supporti magnetici riutilizzabili (*hard drive* esterni, chiavi USB, CD riscrivibili) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (punto 22 del disciplinare tecnico). Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
- I supporti magnetici contenenti dati sensibili e giudiziari (punto 21 del disciplinare tecnico) devono essere custoditi in archivi chiusi a chiave.
- Tutti i supporti magnetici riutilizzabili (*hard drive* esterni, chiavi USB, CD riscrivibili) obsoleti devono essere consegnati all'Amministratore di Sistema per l'opportuna distruzione.
- 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).

ART. 9 UTILIZZO DI *PC* PORTATILI

- L'utente è responsabile del *PC* portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
- Ai *PC* portatili si applicano le regole di utilizzo previste per i *PC* connessi in rete, con particolare attenzione alla rimozione di eventuali *file* elaborati sullo stesso prima della riconsegna.
- I *PC* portatili utilizzati all'esterno (convegni, lavoro domestico autorizzato, ecc…), in caso di allontanamento devono essere custoditi in un luogo protetto.

ART. 10 UTILIZZO DELLE STAMPANTI E DEI MATERIALI DI CONSUMO

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

ART. 11 OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

- È obbligatorio attenersi alle disposizioni in materia di *Privacy* e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato al D.lgs. n. 196/2003.

ART. 12 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:

a) gestire l'*hardware* e il *software* di tutte le strutture tecniche informatiche di appartenenza dell'Istituto, collegate in rete o meno;
b) gestire esecutivamente (creazione, attivazione, disattivazione e tutte le relative attività am-

ministrative) 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;

c) 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;
d) 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;
e) 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;
f) 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;
g) utilizzare le credenziali di accesso di amministrazione del sistema, o l'*account* di un utente tramite re inizializzazione 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.

ART. 13 NON OSSERVANZA DEL REGOLAMENTO

- Si raccomanda il rispetto delle regole contenute nel presente regolamento da parte degli utenti il mancato rispetto o violazione comporterà la revoca delle autorizzazioni e le necessarie conseguenze secondo la normativa vigente, per quanto non previsto nel presente regolamento valgono le disposizioni normative e legislative vigenti.

Art. 14 UTILIZZO LABORATORI DIGITALI - LABORATORI DI INFORMATICA E ATELIER DIGITALI.

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

- 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.

- 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.
- 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*.
- introdurre bevande all'interno dei laboratori di informatica durante l'utilizzo dei *computer* o/e delle stampanti.

L'Amministratore di Sistema

Il Dirigente Scolastico
Dott.ssa Annarita Pintadu