**ITI F. Severi**
Via Luigi Pettinati, 46 35129 Padova (PD)
Tel. 049 8658111 - Fax 049 8658120 email: pdtf04000q@istruzione.it

# MANUALE PRIVACY

Documentazione redatta in ottemperanza a quanto disposto
dal GDPR 2016/679 "*Regolamento generale sulla protezione dei dati*"
e dalla normativa nazionale vigente

**DISCIPLINARE INFORMATICO ISTITUZIONALE**
**Istituto ITI F. Severi**

## Indice

0. Premessa
1. Utilizzo del Personal Computer
2. Utilizzo della Rete Istituzionale
3. Gestione delle Password
4. Utilizzo dei supporti esterni
5. Utilizzo di PC portatili/Tablet
6. Uso della posta elettronica
7. Uso della rete Internet e dei relativi servizi
8. Utilizzo pc portatili/tablet
9. Osservanza delle disposizioni in materia di Privacy
10. Sistemi di controllo graduali
11. Gestione del Sito Internet istituzionale
12. Gestione dei supporti cartacei adibiti ad archiviazione di dati personali.
13. Utilizzo delle apparecchiature tecniche ed elettroniche, inclusa la Rete istituzionale (LAN E WIFI) da parte di terzi.
14. Non osservanza del presente Regolamento

## 0. Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone l'Istituto ITI F. Severi ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Istituto stesso.
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del nostro Istituto deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, l'Istituto ITI F. Severi ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.
Il presente regolamento integra le disposizioni di cui agli artt. 2104 e 2105 codice civile, quelle dei CCNL e delle procedure e regolamenti adottati in Istituto e trova applicazione nei confronti dei dipendenti o di altro personale, anche esterno (da qui in avanti anche detti "utenti"), che, in ragione delle mansioni e/o delle attività assegnate e del lavoro e/o della collaborazione da svolgersi, abbiano in dotazione un personal computer o altro dispositivo con connessione a Internet, nonché una casella di posta elettronica Istituzionale.
Le prescrizioni di seguito previste si aggiungono ed integrano, inoltre, le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del GDPR 2016/679 e dalla normativa nazionale vigente contenente le misure di sicurezza.
Considerato inoltre che l'Istituto ITI F. Severi ha da tempo messo a disposizione del personale docente strumenti affidati in comodato d'uso, si specifica che è consentito un uso personale di questi mezzi esclusivamente fuori dall'orario di lavoro e sotto la totale responsabilità dell'utilizzatore.

## 1. Utilizzo del Personal Computer

1.1 **Segreterie**: Il Personal Computer e, più in generale qualsiasi strumento e/o mezzo informatico, affidato al dipendente è da considerarsi a tutti gli effetti uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete e per lo screen saver. Solo l'Amministratore di sistema e i suoi collaboratori incaricati possono accedere al bios mediante password di attivazione.
Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna, secondo quanto previsto al punto 6 del presente regolamento.

Il dsga potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere allo stesso Istituto, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dallo stesso Istituto, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività dell'Istituto nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.
Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Titolare, dell'Amministratore di sistema o del Delegato Privacy se nominati, in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Titolare e/o dall'Amministratore di sistema. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Istituto a gravi responsabilità civili e 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.
Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del Titolare e/o dell'Amministratore di sistema.
Il Personal Computer (monitor incluso) deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso 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. Eccezione a tale disposizione è rappresentata da una specifica richiesta da parte del Titolare e/o dell'Amministratore di sistema per motivi di manutenzione e/o implementazione del Sistema Informativo medesimo. In ogni caso deve essere attivato lo screen saver e la relativa password.
Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, chiavette UMTS, etc.), se non con l'autorizzazione espressa del Titolare o dell'Amministratore di sistema.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Titolare e/o dell'Amministratore di sistema nel caso in cui vengano rilevati virus.
Tutti i PC devono essere dotati di SOFTWARE ANTIVIRUS aggiornato costantemente e con la funzione "Monitor" attiva.

**1.2. Sala docenti, portinerie, aule, PC docente laboratori, PC sala stampa, PC biblioteca, PC auditorium**: sulle macchine residenti in questi luoghi non dovrà essere conservato nessun dato personale né tantomeno categorie particolari di tipi di dati (es.: valutazioni disabilità, verbali di classe commentati, foto degli studenti, ecc.).

## 2. Utilizzo delle reti ISTITUZIONALI

Le unità di rete sono aree personali o di condivisione d'informazioni strettamente professionali, che non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con nomi utente differenti da quello assegnato.
Il Titolare e/o l'Amministratore di sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza sia sui PC degli incaricati sia sulle unità di rete personali o condivise.
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 cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

## 3. Gestione delle Password

Le password d'ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal Titolare o dall'Amministratore di sistema o da un suo incaricato. E' necessario procedere alla modifica della password a cura dell'incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni tre

mesi; nel caso di trattamento di particolari categorie di dati personali (cosiddetti sensibili o giudiziari) la periodicità della variazione deve essere ridotta a due mesi.
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 devono contenere riferimenti agevolmente riconducibili all'incaricato (è vietato l'uso del proprio nome e/o cognome, di quello dei propri familiari, del proprio luogo e della propria data di nascita e, in generale, di qualsiasi altro riferimento anagrafico).
La password deve essere immediatamente sostituita, dandone comunicazione al Titolare e/o al Amministratore di sistema, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di un altro utente, è tenuto a darne immediata notizia alla al Titolare e/o al Delegato Privacy, ove presente.

## 4. Utilizzo dei supporti esterni

Nel caso in cui siano utilizzati supporti informatici quali chiavette usb, schede SSD, cd-rom o nastri per la memorizzazione di dati personali particolari, gli Incaricati devono osservare alcune misure di sicurezza al fine di salvaguardare la riservatezza dei dati:

- i supporti informatici già contenenti dati personali particolari possono essere riutilizzati solo dopo aver provveduto a cancellare i dati e le informazioni in essi contenuti, in modo che non siano tecnicamente ed in alcun modo recuperabili;
- qualora si riscontrassero delle difficoltà nello svolgimento di tali operazioni, si può richiedere l'intervento dell'Amministratore di Sistema o di un suo incaricato;
- qualora la procedura di cancellazione dei dati risulti inapplicabile, al termine delle operazioni di trattamento i supporti di memoria utilizzati devono essere distrutti;
- fra i supporti di memorizzazione sono ricompresi a pieno titolo i dischi equipaggiati nei computer dismessi e/o sostituiti dai dipendenti.
- non è consentito archiviare nella propria postazione di lavoro, in cartelle personali o condivise, dati strettamente personali.

L'incaricato del trattamento dei dati ha la responsabilità di:

- segnalare la necessità di un'eventuale riparazione degli hard disk;
- segnalare la necessità di un'eventuale dismissione dei CD-ROM, dei nastri magnetici, delle chiavette usb e delle schede SSD;
- eseguire la re-inizializzazione delle chiavette usb e delle schede SSD per poterli successivamente riutilizzare;
- effettuare il test sulla re-inizializzazione delle chiavette usb e delle schede SSD eseguita precedentemente.

Le attività d'uso e riuso sono possibili solo se disposte ed autorizzate specificatamente dal Titolare, dal Delegato Privacy o dall'Amministratore di Sistema e ogni caso non devono in alcun modo pregiudicare I livelli di sicurezza richiesti dall'attività specifica dell'Istituto ITI F. Severi.
I supporti magnetici contenenti dati sensibili e giudiziari devono essere custoditi in archivi chiusi a chiave.

## 5. Utilizzo di PC portatili/TABLET

**PC portatili/Tablet forniti dall'Istituto**: L'utente è responsabile del PC portatile/Tablet 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, in caso di allontanamento dall'Istituto, devono essere custoditi in un luogo protetto e dovranno essere osservate le misure di maggior cautela previste per il collegamento di tali dispositivi, se contengono dati personali in responsabilità all'istituto, nel momento in cui vengano collegati a reti fisiche o wireless non adeguatamente protette secondo quanto stabilito dal GDPR 2016/679 e dalla normativa nazionale vigente.

## 6. Uso della posta elettronica

Il dipendente può accedere alla sua casella di posta elettronica istituzionale, o fornita direttamente dall'Istituto, da tutti gli strumenti che utilizza (*Desktop*, *Laptop*, *Tablet*, *Telefono Mobile*). Gli strumenti dovranno essere dotati dei requisiti di sicurezza definiti dal presente documento; l'Amministratore di sistema può richiedere l'eventuale installazione di appositi applicativi di sicurezza.

Nell'utilizzo del servizio ciascun utente è tenuto a attivare, in caso di assenza prolungata, la funzione di risposta automatica che inviti il mittente a prendere contatto con altre risorse dell'Istituto.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e allegati ingombranti.
l messaggi inviati o ricevuti dall'Utente sono raccolti sul server di posta elettronica Istituzionale (in locale o in remoto), in cui rimangono conservati in base allo spazio di memoria disponibile per la casella assegnata a ciascun utente, secondo le prassi Istituzionali. Tali messaggi sono archiviati automaticamente su sistemi di archiviazione Istituzionale (in locale o in remoto).
Le informazioni contenute nei messaggi di posta elettronica sono da considerarsi riservate e confidenziali. Il loro utilizzo è consentito esclusivamente al destinatario in indirizzo e ne è vietata la diffusione in qualunque modo eseguita, salvo che ne sia data espressa autorizzazione da parte del mittente.
È fatto divieto di utilizzare le caselle di posta elettronica istituzionale per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica Istituzionale per:

- trasmettere a soggetti esterni all'Istituto ITI F. Severi informazioni riservate o comunque documenti Istituzionali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte, per l'adempimento di un obbligo di Legge o di contratto di cui sia parte l'Istituto ITI F. Severi o al fine di difendere un diritto dell'Istituto ITI F. Severi;
- effettuare l'invio e l'archiviazione di messaggi aventi contenuto lesivo per la reputazione dell'Istituto e che gettino discredito sul medesimo o il compimento di qualsiasi atto o fatto illecito attraverso l'utilizzo della casella istituzionale che possano far attribuire all'Istituto ITI F. Severi ed a chi la rappresenta una responsabilità penale, civile od amministrativa;
- effettuare l'invio e l'archiviazione di messaggi di posta elettronica aventi natura oltraggiosa e/o discriminatoria o in ogni caso idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché lo stato di salute e la vita sessuale proprie e/o di terzi;
- effettuare l'invio e l'archiviazione di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa; l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum, chat, social networks o mailing-list estranei all'attività professionale;
- partecipare a catene telematiche (comunemente dette "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, tale attività andrà comunicata immediatamente al Titolare, al Delegato e, ove presente, all'Amministratore di sistema. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
- trasmettere a soggetti interni all'Istituto ITI F. Severi informazioni riservate o comunque documenti Istituzionali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte, per l'adempimento di un obbligo di Legge o di contratto di cui sia parte l'Istituto ITI F. Severi o al fine di difendere un diritto dell'Istituto ITI F. Severi.

Il Delegato Privacy o, ove presente, l'Amministratore di rete e/o i suoi incaricati, qualora ravvedano situazioni particolarmente gravi e/o abusi del servizio, è tenuto ad informare il Dirigente scolastico che provvederà alla contestazione delle mancanze rilevate.
È vietata la consultazione della posta elettronica privata sui dispositivi dati in comodato d'uso dall'Istituto durante l'orario di servizio.

### 7. Uso della rete Internet e dei relativi servizi

Il PC abilitato alla navigazione in Internet costituisce uno strumento dell'Istituto necessario allo svolgimento dell'attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Titolare, dal Delegato Privacy o dall'Amministratore di sistema.
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Dirigente scolastico e con il rispetto delle normali procedure di acquisto.
Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Istituto ITI F. Severi effettua controlli a campione sul volume di dati trasmessi/ricevuti e conserva "file di log" a disposizione delle autorità competenti.

È espressamente vietato:

- accedere ai servizi informatici Istituzionali e/o alle banche dati Istituzionali non possedendo le credenziali di accesso o mediante l'utilizzo delle credenziali di colleghi autorizzati;
- l'installazione, la configurazione e l'utilizzo di software "Peer-To-Peer" (P2P tipo eMule, Torrent e

similari) il quale, oltre a saturare le risorse di banda internet disponibili, è veicolo di potenziali e gravissimi rischi per la sicurezza del sistema informatico Istituzionale; può altresì comportare il concreto rischio di scarico di materiale illegale (v. Legge sul Diritto d'Autore) e/o pedo-pornografico;

- la navigazione su siti appartenenti alle categorie Pedo/Pornografia, Violenza, Razzismo, estremismo politico e religioso e, in generale, è espressamente vietata la navigazione e ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate;
- accedere in maniera non autorizzata ai sistemi informativi della pubblica amministrazione o alterarne in qualsiasi modo il funzionamento o intervenire con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi contenuti in sistema informatico o telematico o a questo pertinenti, per ottenere e/o modificare informazioni a vantaggio dell'Istituto o di terzi o comunque al fine di procurare un indebito vantaggio all'Istituto od a terzi;
- distruggere, deteriorare o rendere inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati utilizzati dallo Stato o da altro ente pubblico o ad esso pertinente o comunque di pubblica utilità;
- condurre, in una qualsiasi forma, attacchi telematici a terzi e/o strutture e/o strumenti digitali a loro appartenenti e, più in generale, qualsiasi azione in violazione delle leggi e delle normative vigenti in materia di Diritto della Privacy, dell'Informatica e delle Telecomunicazioni.

## 8. Utilizzo pc portatili/tablet

PC portatili:
I pc portatili in dotazione per l'uso lavorativo non possono essere ceduti né fatti utilizzare a terzi.
Non è consentito modificare le caratteristiche hardware e software impostate sui dispositivi mobili.
Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Titolare o dall'Amministratore di rete, ove presente.
Non è consentita la riproduzione, la duplicazione, il salvataggio, la condivisione o lo scarico (download o file sharing) di programmi o file di ogni tipo (testo, immagini, video, audio, eseguibili) in violazione delle norme sul diritto d'autore, ai sensi delle Legge n. 128 del 21 maggio 2004.
Non è consentito l'uso di qualsiasi dispositivo esterno collegabile, se non quelli istituzionali o autorizzati.
L'utilizzatore che abbia necessità di apportare modifiche software o hardware, installando nuovi programmi o periferiche, deve farne preventiva richiesta all'Amministratore di sistema.
Quanto memorizzato sui supporti interni al dispositivo potrebbe essere oggetto di analisi, controllo e duplicazione da parte dell'Amministratore di sistema o da personale tecnico autorizzato, per migliorare l'affidabilità, la disponibilità e l'efficienza del dispositivo.
Qualora fossero individuate componenti hardware e/o software (programmi, documenti, dispositivi esterni, etc.) non corrispondenti ai criteri di sicurezza e di operatività o non esplicitamente autorizzati, tali componenti potranno essere rimossi e l'utilizzatore essere coinvolto negli accertamenti del caso.

### 8.1 Disposizioni operative

- I pc portatili devono avere abilitata la Password personalizzata. Si consiglia l'uso di password alfanumeriche composte anche di lettere maiuscole e simboli.

### 8.2 Disposizioni operative per i Tablet

- I dispositivi *mobile* devono essere dotati di software antivirus aggiornabile automaticamente e con la funzione di monitoraggio attiva.
- Nel caso di dispositivi tablet, è fatto divieto di utilizzare qualsiasi software e/o tecnica di jailbreak (Apple) o root (Android), cioè di quei sistemi che consentono di modificare funzionalità del sistema operativo di un dispositivo a basso livello ed a livello di "massimo amministratore".

### 8.3 Guasto o furto

In caso di guasti o malfunzionamenti, l'utilizzatore dovrà rivolgersi all'Amministratore di sistema o a un suo incaricato, a cui è demandata la gestione in queste circostanze.
In caso di furto o smarrimento o danneggiamento dei dispositivi in comodato, l'utilizzatore deve dare tempestiva comunicazione all'Amministratore di Sistema e/o al Titolare, rimanendo a disposizione nel caso sia necessario denunciare l'accaduto all'Autorità preposta.
Non è esclusa a priori la responsabilità dell'utilizzatore nel sostenere, anche solo in parte, i costi per la riparazione o sostituzione del dispositivo.

Si ricorda che l'obbligo di conservazione dei dati personali contenuti nel dispositivo mobile è in carico ai rispettivi utilizzatori.

## 9. Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del GDPR 2016/679.
Poiché in caso di violazioni contrattuali e giuridiche, sia l'Istituto, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Istituto verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

Ai sensi dell'art. 13 e 14 del GDPR 2016/679, in conformità a quanto disposto dalla Provvedimento n. 13 del 1° marzo 2007 dell'Autorità Garante per la privacy, si ritiene necessario informare che:

- Il Dirigente scolastico, attraverso l'Amministratore di Sistema, effettua un monitoraggio periodico dell'hardware e del software installato nei dispositivi informatici. Tale operazione viene effettuata in modo completamente automatico per i dispositivi ed i sistemi operativi che lo consentono ed in modo manuale per tutti gli altri. Il monitoraggio, necessario per finalità organizzative (inventario del parco macchine e contabilità delle licenze d'uso del software), non coinvolge in alcun modo i dati personali ed i documenti presenti sui dispositivi, ma permette la rilevazione di software installato in violazione di questo Disciplinare.
- L'Amministratore di Sistema può accedere alle cartelle personali e condivise per contrasto virus, malware, intrusioni telematiche, fenomeni quali *spyware*, ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione *hardware*). Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, l'Amministratore di Sistema o il suo incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo.
- Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, l'Amministratore di Sistema avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni, attraverso strumenti adeguati. Lo stesso Amministratore di Sistema e/o i suoi incaricati possono, nei casi su indicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico Istituzionale (ad es. rimozione di file o applicazioni pericolosi).
- In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica delle caselle nome.cognome@itiseveripadova.edu.it, l'utente può formalmente delegare un altro lavoratore (Fiduciario, così come definito dal Provvedimento del Garante della Privacy Nr. 13 del 1 marzo 2007 "*Lavoro: le linee guida del Garante per posta elettronica e internet"*) e del 27 novembre 2008 ("*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*) a verificare il contenuto dei messaggi, a gestire le strette necessità operative e/o ad inoltrare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. In assenza della nomina di un fiduciario, da effettuarsi entro tempi adeguati all'espletamento della richiesta avanzata da parte del Titolare, con la presenza di quest'ultimo e di personale appositamente incaricato (ad esempio l'Amministratore di sistema o i suoi incaricati), il Titolare o persona da lui delegata, può legittimamente verificare il contenuto dei messaggi al fine di estrarre le informazioni ritenute rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività verrà redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile.
- Al fine di prevenire, per quanto e ove possibile, comportamenti scorretti durante la navigazione in Internet, l'Istituto raccoglie e conserva "file di log" a disposizione delle autorità competenti.
- L'eventuale controllo sui *file* di *log* da parte dell'Amministratore di Sistema non è comunque continuativo ed è limitato ad alcune informazioni (es. Navigazione Internet: il nome dell'utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità di sicurezza dell'Istituto, e comunque non oltre 6 mesi, fatti salvi in ogni caso specifici obblighi di legge. Eventuali comportamenti anomali saranno segnalati al Dirigente scolastico.
- L'Amministratore di Sistema e i suoi incaricati sono altresì abilitati ad accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'Istituto per cessazione del rapporto, sostituzione delle apparecchiature, etc.

Il trattamento dei dati, così come descritto, è obbligatorio, pena l'impossibilità di utilizzare qualunque dispositivo informatico, digitale e/o mobile.
L'Istituto ITI F. Severi garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinato al controllo a distanza.
Nell'ambito delle misure di controllo del livello di sicurezza del sistema informativo, è possibile che il Titolare o l'Amministratore di Sistema, effettui tentativi di violazione delle *password* degli utenti. Nel caso il tentativo abbia esito positivo, verrà chiesto all'utente di sostituire immediatamente la *password*.

## 10. Sistemi di controllo graduali

In caso di anomalie, l'Amministratore di Sistema effettuerà controlli preliminari su dati aggregati, riferiti all'intera struttura lavorativa o a singoli settori (es. sala insegnanti, laboratorio X) che si concluderanno con avvisi generalizzati diretti ai dipendenti operanti nei settori in cui sia stata rilevata l'anomalia, per evidenziare l'utilizzo irregolare degli strumenti Istituzionali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie (come previsto dal p. 6.1 della Delibera Nr. 13 del 1/3/2007 Garante Privacy "*Lavoro: le linee guida del Garante per posta elettronica e internet"*). In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

## 11. Gestione del Sito Internet istituzionale

La gestione, in qualità di amministratore, del sito internet istituzionale, viene attribuita con incarico da parte del Titolare del Trattamento. Tutti i contenuti devono essere valutati secondo i principi di pertinenza e non eccedenza, secondo quanto stabilito nel PTOF relativamente agli ambiti strettamente didattico/istituzionali, con attenzione alle modalità di pubblicazione e sicurezza (deindicizzazione delle pagine o utilizzo di aree riservate), alla trasparenza, secondo quanto previsto esclusivamente da una Legge o da un regolamento o per scopi strettamente istituzionali.
Si ricorda che la pubblicazione di qualsiasi tipo di dati personali (anche solo il nome e cognome di un soggetto), se non prevista per Legge o da Regolamento, è vietata.
Deve essere sempre controllata e, se necessario, aggiornata, la documentazione del sito necessaria all'adeguamento con quanto disposto dal GDPR 2016/679 e dalla normativa nazionale vigente.
Eventuali siti al di fuori del dominio istituzionale (.edu.it) dovranno essere impostati come sottodomini del dominio istituzionale stesso (es.: www.itiseveripadova.edu.it) e non in maniera isolata.
È vietato concedere l'uso a terzi del logo, del nome e di qualunque altro dato che possa indebitamente ricondurre ad una responsabilità diretta dell'Istituto (es. siti/blog/social privati dei docenti, comitati genitori, ecc.)

## 12. Gestione dei supporti cartacei adibiti ad archiviazione di dati personali.

Il corretto utilizzo dei supporti cartacei (temi in classe, verbali, appunti, quaderni) sia in responsabilità all'Istituto che ad uso privato del personale (es. docenti), è sotto la diretta ed esclusiva responsabilità del legittimo proprietario e/o utilizzatore, inclusi gli obblighi di riservatezza già previsti per il corpo docente e per tutti coloro che lavorano all'interno dell'Istituto stesso, riguardo sia al segreto d'ufficio e professionale, sia relativi alla conservazione dei dati personali eventualmente contenuti nei predetti supporti (ex art. 2050 del C.C.); di conseguenza l'Istituto non potrà essere ritenuto responsabile in nessun modo per un utilizzo inadeguato o indebito, da parte dei rispettivi utilizzatori e/o proprietari, dei predetti strumenti.

## 13. Utilizzo delle apparecchiature tecniche ed elettroniche, inclusa la Rete istituzionale (LAN E WIFI) da parte di terzi.

L'utilizzo della strumentazione tecnica, tecnologica nonché dell'infrastruttura di rete, sia fisica (Lan) che logica (WiFi), è consentita a terzi solo previa autorizzazione da parte del Dirigente scolastico. Di conseguenza il personale interessato, una volta avuta l'autorizzazione, al fine di concedere l'uso di tali strumenti a terzi, dovrà avere cura di far firmare gli appositi moduli di richiesta reperibili presso gli incaricati dell'Amministratore di Sistema e di verificare che negli eventuali supporti di memorizzazione non siano presenti dati personali.

## 14. Non osservanza del presente Regolamento

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonchè con le azioni civili e penali consentite.

L'Istituto ITI F. Severi