**ISTITUTO COMPRENSIVO STATALE di CASIER**

Scuola Primaria – Scuola Secondaria di 1° grado – Via Peschiere, 16 - 31030 DOSSON DI CASIER (TV)
Tel. 0422 380848/491560 - Cod. meccanografico: TVIC82300C
✉ mail: info@iccasier.edu.it - Pec: TVIC82300C@PEC.ISTRUZIONE.IT – Web: www.iccasier.edu.it
C/C/P 17097312 – Cod. Fisc. 80017580269 - IBAN: IT 79 J 01030 61960 000000649878


# REGOLAMENTO SULL'USO DI STRUMENTAZIONI,

# DI INTERNET

# E DELLA POSTA ELETTRONICA

(POLICY DELLA SCUOLA)

**Vista** la legge 20 maggio 1970 n. 300 "*Statuto dei Lavoratori*";

**Viste** la Legge 7 agosto 1990 n. 241 "*Nuove norme in materia di procedimento amministrativo e di diritto* di accesso ai documenti amministrativi" e la Legge 11 febbraio 2005 "*Modifiche ed integrazioni alla legge 7/8/90 n. 241 concernenti norme generali sull'azione amministrativa";*

**Visto** il D. Lgs. n. 242 del 19 marzo 1996 "*Modifiche ed integrazioni al decreto legislativo 19 settembre 1994, n. 626, recante attuazione di direttive comunitarie riguardanti il miglioramento della sicurezza e della salute dei lavoratori sul luogo di lavoro*".

**Visto** il DPR del 28 dicembre 2000 n. 445 "*Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"*

**Visto** il D. Lgs. del 30 giugno 2003 n. 196 "*Codice in materia di protezione dei dati personali" e sue ss.mm.ii.;*

**Vista** la deliberazione del CNIPA 19 dicembre 2004 n. 11 "*Regole tecniche dei documenti digitali*";

**Visto** il D. Lgs. 7 marzo 2005 n. 82 "*Codice dell'Amministrazione Digitale*";

**Visto** il S.O. n. 93 aggiornato dal D. Lgs. 159 del 4 aprile 2006 recante "*Disposizioni integrative e correttive al D. Lgs. 7 marzo 2005 n. 82;*

**Visto** il D.M. del 7 dicembre 2006, n. 305 "*Regolamento recante identificazione dei dati sensibili e giudiziari";*

**Visto** il Provvedimento del 01 marzo 2007 "Linee guida del Garante per posta elettronica e internet";

**Vista** la Direttiva del Consiglio dei Ministri n. 2/2009 del 26/05/2009;

**Visto** il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

**Vista** la Direttiva UE 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati;

**Ritenuto** opportuno richiamare gli artt. 2086, 2087 e 2014 del Codice Civile;

**Considerato** che l'Istituto Comprensivo Statale di Casier tra i vari strumenti di lavoro ha messo a disposizione dei dipendenti e studenti accessi ad Internet e servizi di caselle di posta elettronica per lo svolgimento delle mansioni e compiti loro affidati;

**Richiamato** il principio generale che l'utilizzo delle risorse ICT che la scuola mette a disposizione dei dipendenti deve sempre ispirarsi a criteri di diligenza e correttezza normalmente adottati nell'ambito dei rapporti di lavoro;

**Rilevato** che l'Autorità Garante per la Privacy, con delibera n. 13 del 1.3.2007 (pubblicata in G.U. del 10.3.2007 n. 58) ha inteso precisare che è opportuno da parte dei Datori di Lavoro

adottare un disciplinare interno redatto in modo chiaro, senza formule generiche ed adeguatamente pubblicizzato verso i singoli dipendenti interessati, anche ai fini dell'esercizio del potere disciplinare;

**Ritenuto** che l'adozione del Regolamento consente di escludere l'applicabilità della normativa penale a tutela della corrispondenza elettronica poiché, essendo considerata strumento di lavoro, non può essere considerata corrispondenza privata;

**Considerato**, inoltre, che, se correttamente applicato e fatto rispettare, il Regolamento può risultare un efficace strumento della Policy scolastica anche al fine di limitare il rischio di insorgenza di responsabilità amministrativa della Scuola;

**Ritenuto**, pertanto, di dover adottare apposito Regolamento per l'utilizzo di Internet e della Posta Elettronica in cui è, tra l'altro, precisato che gli stessi sono strumenti aziendali e come tali soggetti anche a controlli secondo i principi ed i criteri di cui ai commi 5, 6 e 7 del citato Provvedimento del Garante e della normativa in tema di Protezione dei dati personali;

**Tenuto conto** che il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, a tutti i collaboratori della scuola, interni od esterni, ai collaboratori a progetto ed a quelli durante il periodo di stage, a prescindere dal rapporto contrattuale con la stessa intrattenuto, nonché agli alunni;

viene disposto il seguente

**Disciplinare per l'utilizzo della strumentazione, della rete internet e della posta elettronica.**

***Versione del documento***

| N° | Descrizione | Emesso | Approvato |
|---|---|---|---|
| 1.0 | Prima emissione | 27/01/2019 | 26/01/2019 |
| 2.0 | Adeguamento a REG UE 2016/679 | 18/09/2019 | |

# SOMMARIO

# PREMESSA

L'uso improprio degli strumenti che l'Istituto mette a disposizione per il trattamento dei dati e delle informazioni, oltre ad arrecare un danno in termini di maggiori costi e possibili perdite di continuità del servizio, può nuocere allo stesso da un punto di vista della reputazione e condurre a procedimenti legali con sanzioni di tipo amministrativo e penale.
Poiché la sicurezza dei dati non dipende solo da aspetti tecnici, ma anche, se non principalmente, da quelli organizzativi e comportamentali, tutti i dipendenti devono considerarla una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione.
Anche la vigente normativa in materia di protezione dei dati personali e i Provvedimenti del Garante Privacy impongono, per procedere ad ogni trattamento dei dati personali, l'adozione e il rispetto di certi criteri guida nel trattamento dei dati.

Quale complemento e integrazione della sicurezza, è necessario quindi adottare e diffondere nell'Istituto una politica trasparente in cui siano esplicitati i limiti di utilizzo delle risorse assegnate ai dipendenti per lo svolgimento delle mansioni lavorative nonché le regole comportamentali da osservare per trattare in modo sicuro sia i dati informatici che quelli cartacei.
L'adozione di queste politiche viene fatta nell'intento di:

- provvedere ad un servizio continuativo nell'interesse dell'Istituto
- salvaguardare la riservatezza delle informazioni e dei dati
- tutelarsi da potenziali responsabilità legali
- proteggere il buon nome e l'immagine dell'Istituto
- proteggere gli investimenti effettuati
- evitare problemi di sicurezza informando e incentivando i comportamenti corretti
- garantire la massima efficienza delle risorse informatiche e del loro utilizzo
- contribuire al rispetto delle norme sul trattamento di dati personali.

# FINALITÀ DEL DOCUMENTO

Il presente Regolamento viene incontro alla necessità di disciplinare il trattamento di dati personali e le condizioni per il corretto utilizzo dei beni dell'Istituto in applicazione dei principi di cui alla vigente normativa in materia di protezione dei dati personali.
L'Istituto intende contribuire alla massima diffusione della cultura della sicurezza per evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla riservatezza-sicurezza nel trattamento dei dati.
Disciplina pertanto le modalità di accesso e di uso delle strumentazioni, della rete informatica, telematica e dei servizi che, tramite la rete stessa, è possibile ricevere o offrire all'interno e all'esterno dell'Istituto per dare il supporto informativo documentario alla ricerca, alla didattica, all'aggiornamento e alle attività collaborative tra scuole ed enti, nonché per tutti gli adempimenti amministrativi di legge.

## AMBITO DI APPLICAZIONE

La rete dell'Istituto è costituita dall'insieme delle risorse informatiche, cioè:
-dalle componenti hardware/software e dagli apparati elettronici collegati alla rete informatica dell'Istituto,
-dall'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.
Il presente Regolamento si applica, senza distinzione di ruolo e/o livello, a tutti gli utenti interni (personale amministrativo, docenti e collaboratori scolastici) autorizzati ad accedere alla rete della scuola nell'ambito della propria attività lavorativa ordinaria e straordinaria e agli studenti nei limiti loro assegnati a scopi didattici ed educativi.
Analogamente il presente Regolamento si applica alla ditta che effettua attività di manutenzione e agli altri eventuali soggetti esterni autorizzati all'accesso a specifiche banche dati e a tutti i collaboratori dell'istituto a prescindere dal rapporto contrattuale con gli stessi intrattenuto (es. soggetti in attività di stage, relatori e formatori per corsi di aggiornamento, ...).

## PRINCIPI GENERALI

L'istituto prevede l'utilizzo delle strumentazioni informatiche, della rete internet e della posta elettronica da parte degli utenti quali strumenti utili a perseguire le proprie finalità istituzionali eprevede che lo stesso si conformi ai seguenti principi:
-principio di necessità: i sistemi informativi e i programmi informatici vengono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
-principio di correttezza: le caratteristiche essenziali dei trattamenti sono rese note agli utenti;
-principio di pertinenza e non eccedenza: i trattamenti sono effettuati per finalità determinate, esplicite e legittime e i dati sono trattati nella misura meno invasiva possibile.
Per assicurare la tutela dei diritti, delle libertà fondamentali e della dignità dei lavoratori, garantendo che sia assicurata una ragionevole protezione delle loro sfera di riservatezza nelle relazioni personali professionali, il trattamento dei dati mediante l'uso delle tecnologie telematiche è conformato al rispetto dei diritti delle libertà fondamentali nonché della dignità dell'interessato, dei divieti posti dallo statuto dei lavoratori sul controllo a distanza e dei principi di necessità, correttezza e finalità determinate, esplicite e legittime.
Ogni utente è responsabile, sia sotto il profilo civile che penale, del corretto uso delle risorse informatiche, dei servizi e dei programmi ai quali ha accesso e dei dati che tratta.
Spetta ai docenti vigilare affinché gli studenti loro affidati rispettino il regolamento e sono ne direttamente responsabili.

# DEFINIZIONI

1. “trattamento”, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
2. “dato personale”, qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
3. “dati c.d. identificativi”, i dati personali che permettono l'identificazione diretta dell'interessato (nome, cognome, codice fiscale, indirizzo e-mail...);
4. “dati c.d. sensibili”, i dati personali 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, i dati personali idonei a rivelare lo stato di salute e la vita sessuale, i dati genetici, i dati biometrici;
5. “titolare”, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
6. “c.d. incaricati”, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
7. “interessato”, la persona fisica cui si riferiscono i dati personali;
8. “comunicazione”, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
9. “diffusione”, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
10. "Garante Privacy", l'autorità per la Protezione dei dati personali con compiti di vigilanza, indirizzo, informazione, promozione, consultazione e dotata di poteri ispettivi e sanzionatori.

# VALUTAZIONE DEL RISCHIO

La rete informatica di Istituto, l’accesso alla rete internet e alla posta elettronica, la strumentazione affidata al dipendente sono strumenti di lavoro; su di essi vengono effettuate regolari attività di controllo, amministrazione e back up ed essi non possono in alcun modo essere utilizzati per scopi diversi perché ogni utilizzo non inerente all’attività lavorativa può contribuire ad innescare disservizi, costidi manutenzione e, soprattutto, minacce alla sicurezza.

In relazione all'utilizzo non corretto di detti strumenti si individuano i seguenti possibili rischi econseguenti effetti, rappresentati nella tabella sottostante:

| Attività | Rischio | Motivazione | Possibile effetto |
|---|---|---|---|
| Manutenzione di periferiche hardware interne (scheda video, ecc.) | Alto | Possono essere danneggiati componenti interne e il PC | Danneggiamento della strumentazione |
| Manutenzione di periferiche hardware esterne (tastiera, mouse, ecc.) | Basso | | Limitazione nell'utilizzo |
| Download non controllato o non programmato di aggiornamenti relativi ad applicazioni installatedal responsabile di rete | Alto | Possono essere scaricate applicazioni non verificate con il pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore | Danneggiamento del software del PC o della rete informatica interna |
| Download controllato o programmato di aggiornamenti relativi ad applicazioni installate dal responsabile di rete | Basso | | |
| Download di dati non inerenti alle attività lavorative (musica, giochi, ecc.) | Alto | Possono essere scaricate applicazioni non verificate con il pericolo di portare virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore | Danneggiamento del software del PC o della rete informatica interna. Gravi responsabilità civili epenali per l'Istituto in caso di violazione della normativa a tutela dei diritti d'autore |
| Installazione di applicazioni senza l'autorizzazione del responsabile della rete | Alto | Possono essere installate applicazioni non compatibili | Danneggiamento del software del PC o della rete informatica interna |
| Accesso alla rete effettuato da Pcdi proprietà dell'utente | Alto | Accessi non autorizzati alla rete | Furto di dati |
| Apertura di allegati di posta elettronica di incerta provenienza | Alto | Possono contenere Malware/Spyware | Danneggiamento del software del PC o della rete informatica interna. |

| | | | |
|---|---|---|---|
| | | | Divulgazione di password e dati riservati |
| Elaboratore connesso alla rete lasciato incustodito o divulgazione di password | Alto | Possibile utilizzo da parte di terzi | Uso indebito di dati riservati, danneggiamento della rete informatica interna |
| Utilizzo di supporti removibili esterni non autorizzati | Alto | Possono essere trasferite applicazioni dannose per il PC nella rete informatica | Danneggiamento dei PC o della rete informatica interna |
| Furto di dati<br>Mancata distruzione o perdita accidentale di supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi usb, cd riscrivibili, ...) contenenti dati sensibili e giudiziari | Alto | Recupero di dati memorizzati anche dopo la loro cancellazione | Uso indebito di dati riservati |

# CIRCOLAZIONE INTERNA E COMUNICAZIONE DEI DATI

## CIRCOLAZIONE INTERNA DEI DATI

L'accesso ai dati personali da parte dei dipendenti dell'IC di Casier comunque limitato ai casi in cui sia necessario al perseguimento dei fini dell'Istituto, è ispirato al principio della libera circolazione delle informazioni all'interno dell'Istituto.
Ogni richiesta d'accesso ai dati personali da parte dei dipendenti dell'IC di Casier, purché connessa con lo svolgimento dell'attività inerente alla specifica funzione del richiedente (ambito del trattamento), deve essere soddisfatta in via diretta, senza formalità, nella misura necessaria al perseguimento dell'interesse dell'Istituto.

Laddove la richiesta da parte dei dipendenti fosse finalizzata ad un utilizzo ulteriore e/o diverso dei dati, sarà necessario, da parte di questi soggetti, presentare una richiesta scritta e motivata.
Chi richiede i dati, chi li riceve, chi li tratta e chi ne ha notizia è vincolato al rispetto del segreto d'ufficio. La responsabilità, anche penale, per l'uso non corretto dei dati personali conosciuti resta a carico della singola persona cui l'uso illegittimo si riferisca.

L'utilizzo dei dati personali deve avvenire in base al principio del "*need to know*" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). I dati possono essere comunicati all'esterno esclusivamente ai soggetti e nei modi indicati nell'informativa sul trattamento dei dati rilasciata dell'IC di Casier.
La comunicazione di dati personali da parte dell'Istituto è effettuata in esecuzione di obblighi di legge e per le sole finalità indicate nell'informativa per il trattamento dei dati personali rilasciata dell'IC di Casier.
Una volta verificata la sussistenza di tali prerequisiti, prima di effettuare la comunicazione dei dati occorrerà in ogni caso:

- accertarsi dell'identità del soggetto a cui i dati vengono comunicati
- verificare l'esattezza dei dati comunicati.

Non è consentito fornire informazioni telefoniche contenenti dati personali a chicchessia, ivi comprese amministrazioni pubbliche o autorità giudiziarie.

Particolare attenzione va riposta in caso di domande/interviste telefoniche cui si raccomanda di non rispondere oppure di rispondere solo dopo ricevimento di nota informativa scritta (lettera, fax, e-mail) che consenta di verificare l'identità e il titolo del richiedente nonché le finalità della richiesta.

Massima cautela deve essere applicata anche nell'invio di informazioni a mezzo fax, pertanto occorrerà prestare attenzione a:

- digitare correttamente il numero di fax del destinatario;
- controllare l'esattezza del numero prima di inviare il documento;
- stampare il rapporto di trasmissione verificando (ove ricevuto) l'identificativo del numero chiamato.

# NOMINA DELL'AMMINISTRATORE DI SISTEMA E DEL CUSTODE DELLE PASSWORD

Il datore di lavoro conferisce all'**Amministratore di sistema** il compito di sovrintendere alle risorse informatiche dell'Istituto assegnandogli in maniera esclusiva le seguenti attività:
a) gestione dell'hardware e del software (installazione, aggiornamento, rimozione) di tutte le strutture tecniche informatiche dell'istituto, siano esse collegate in rete o meno;
b) configurazione dei servizi di accesso alla rete interna, ad internet e a quelli di posta elettronica con creazione, attivazione e disattivazione dei relativi account;
c) attivazione della password di accensione (BIOS);
d) creazione di un'area condivisa sul server per lo scambio di dati tra i vari utenti, evitando condivisioni dei dischi o di altri supporti configurati nel PC che non siano strettamente necessarie;
e) controllo del corretto utilizzo delle risorse di rete, dei computer e degli applicativi, durante le 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) rimozione sia sui PC degli incaricati sia sulle unità di rete, di ogni tipo di file o applicazione che possa essere pericoloso per la sicurezza o costituisca violazione del presente regolamento;
g) distruzione delle unità di memoria interne alla macchina (hard - disk, memorie allo stato solido) ogni qualvolta si procederà alla dismissione di un PC e dei supporti removibili;
h) utilizzo delle credenziali di amministrazione del sistema per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di indispensabile ed indifferibile necessità di intervento per prolungata assenza, irrintracciabilità o impedimento dello stesso, solo per il tempo necessario al compimento di attività indifferibili e solo su richiesta del Responsabile del trattamento.
L'Amministratore di sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, al PC di ciascun utente.
Il **Custode delle password** è incaricato di custodire e conservare in luogo riservato e sicuro, in formato cartaceo, le credenziali.
E' tenuto a ottemperare al suo compito avendo cura di non diffondere, nemmeno accidentalmente, le stesse a persone estranee al loro utilizzo.

# SICUREZZA FISICA

La sicurezza fisica è l'insieme delle misure di protezione fissate per impedire l'accesso fisico di terzi non autorizzati ai dati, cartacei o informatici.

E' responsabilità dell'utente:

- provvedere alla custodia delle apparecchiature in dotazione utilizzandole in modo adeguato, eventuali danneggiamenti, smarrimenti o furti dovranno essere comunicati immediatamente al Dirigente;
- mantenere i propri supporti di memorizzazione (CD, DVD, floppy, device USB, ecc.) in luogo appropriato e possibilmente non in vista quando non sono utilizzati; se contengono dati riservati o personali ai sensi delle leggi vigenti in materia di privacy, dovranno essere custoditi in armadi o cassetti chiusi a chiave;
- tenere lontani i supporti di memorizzazione da rischi ambientali come calore eccessivo, luce solare diretta e campi magnetici;
- evitare di esporre l'hardware a condizioni estreme di umidità e/o temperatura o a contatti con liquidi, fumo ecc.;
- tener conto dei rischi derivanti da eventi straordinari dovuti a cause naturali (come incendi, allagamenti, ecc.);
- procedere a spostamenti, disconnessioni, reinstallazioni, ecc. delle apparecchiature in dotazione solo con l'autorizzazione del Dirigente;
- trasportare fuori dall'Istituto le apparecchiature portatili condivise con altri utenti (es.: un portatile non in dotazione stabile) solo con il consenso del Dirigente;
- conservare documenti contenenti dati personali in locali non accessibili a terzi non autorizzati;
- assicurarsi che l'accesso alle aree ove sono custoditi dati sia controllato visivamente da qualcuno o che le stesse aree siano chiuse a chiave;
- fare attendere soggetti terzi in luoghi in cui non siano presenti informazioni riservate o dati personali;
- chiudere le finestre e le porte al termine delle attività lavorative o comunque quando gli uffici non sono presidiati;

- riporre i documenti ed effettuare la disconnessione del proprio PC o attivarne il salvaschermo con password quando è necessario allontanarsi dalla scrivania.

# TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

E' responsabilità dell'utente seguire le istruzioni di seguito esposte.

## ISTRUZIONI PER LA CUSTODIA DI DATI PERSONALI

- Gli atti e i documenti contenenti dati personali devono essere controllati e custoditi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione;
- al termine delle operazioni di trattamento riporre gli atti e i documenti negli archivi;
- gli atti e i documenti contenenti dati personali sensibili o comunque riservati per l'Istituto devono essere conservati in armadi o cassetti dotati di serratura;
- i dati idonei a rivelare lo stato di salute devono essere conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo;
- non lasciare sparsi sulle scrivanie o appoggiati su ripiani o in luoghi in cui siano visibili a terzi non autorizzati (che possono venirne a conoscenza e divulgarli) atti e documenti cartacei (anche lettere o comunicazioni pervenute tramite la posta o a mezzo telefax);
- fotocopie o copie di documenti devono essere custodite con le stesse modalità dei documenti originali;
- in caso di utilizzo di stampanti condivise o collocate in spazi comuni, i documenti cartacei dovranno essere prelevati immediatamente dopo la stampa.

## ISTRUZIONI PER LA DISTRUZIONE DI DATI PERSONALI

Qualora sia necessario distruggere i documenti contenti dati personali, la distruzione definitiva deve avvenire in modo controllato ed in modalità tale da assicurare il non riutilizzo dei dati (ad esempio utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, essere sminuzzati in modo da non essere più ricomponibili).
I supporti rimovibili contenenti dati sensibili se non utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

## ISTRUZIONI PER IL TRATTAMENTO DI DATI SENSIBILI

L'archiviazione dei documenti cartacei contenenti dati sensibili deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.

# TRATTAMENTI CON L'AUSILIO DI STRUMENTI ELETTRONICI

## SICUREZZA LOGICA

La sicurezza logica è l'insieme delle misure di protezione stabilite per assicurare che gli accessi ai sistemi informativi avvengano secondo modalità predefinite, tali da garantire un elevato livello di robustezza ed affidabilità.
A tal scopo è necessario identificare gli utenti che accedono ai sistemi informatici utilizzati per il trattamento dei dati.

## ASSEGNAZIONE DELLE POSTAZIONI DI LAVORO

Per ridurre il rischio di impieghi abusivi o dannosi, il datore di lavoro provvede a:
-individuare preventivamente le postazioni di lavoro e assegnarle a ciascun dipendente,
-individuare preventivamente gli utenti a cui è accordato l'utilizzo della posta elettronica e l'accesso a internet.
La strumentazione dell'Istituto non è di esclusivo dominio del dipendente, ma rientra tra i beni a cui determinati soggetti possono comunque sempre accedere. L'eventuale accesso del datore di lavoro, qualora necessiti di informazioni contenute nei documenti residenti sul PC assegnato al dipendente, è legittimo.

## UTILIZZO DEI PERSONAL COMPUTER

Gli utenti utilizzano per il proprio lavoro soltanto computer di proprietà dell'Istituto di cui sono responsabili, salvo eccezioni richieste ed autorizzate dal Dirigente Scolastico e dall'Amministratore di sistema.
Sono tenuti a:

- applicare al PC portatile le regole di utilizzo previste per i PC connessi in rete,
- custodirlo con diligenza e in luogo protetto durante gli spostamenti,
- rimuovere gli eventuali file elaborati sullo stesso prima della sua riconsegna,
- non disattivare sul PC lo screen saver e la relativa password,
- conservare la password nella massima riservatezza e con la massima diligenza,
- non modificare la configurazione hardware e software del PC se non esplicitamenteautorizzati dall'amministratore di sistema,
- non rimuovere, danneggiare o asportare componenti hardware,
- nel caso il software antivirus rilevi la presenza di un virus, sospendere immediatamente ognielaborazione in corso, senza spegnere il PC e segnalare prontamente l'accaduto al personaleincaricato dell'assistenza tecnica,
- permettere l'autoaggiornamento del PC,

- prestare la massima attenzione ai supporti di origine esterna (es. pendrive), verificando preventivamente, tramite il programma antivirus, ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l'Amministratore di sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti,
- non lasciare incustodita e accessibile la propria postazione una volta eseguita la connessione al sistema conle proprie credenziali di autenticazione,
- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso ad internet e ai servizi di posta elettronica,
- spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.
- trasportare fuori dall'Istituto le apparecchiature portatili condivise con altri utenti (es.: un portatile non in dotazione stabile) solo con il consenso del Dirigente;
- conservare documenti contenenti dati personali in locali non accessibili a terzi non autorizzati;
- navigare in siti che possono rivelare le opinioni politiche, religiose o sindacali del dipendente;
- accedere a siti web dal contenuto offensivo, pornografico, discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o comunque illegale in qualsiasi formato (programmi, immagini, testi, video, suoni, …)
- memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- scaricare files di grandi dimensioni ed effettuare navigazioni ad elevato consumo di banda, se non espressamente autorizzato dal Dirigente;
- scaricare software gratuiti (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Dirigente;
- ascoltare, sui *PC* dotati di scheda audio e/o di lettore CD, programmi, *files* audio o musicali, se non a fini prettamente lavorativi;
- Riprodurre o duplicare programmi informatici ai sensi delle Legge n. 128 del 21/05/2004;
- Collegare pc portatili o altri dispositivi mobili non dell'Istituto alla rete, salvo autorizzazione del Dirigente.

Si ricorda che quanto più il desktop è occupato da icone, file o anche solo da collegamenti, tanto più lento sarà il caricamento del profilo all'avvio, ad esempio al mattino al momento dell'accensione.
Pertanto si raccomanda di mantenere pulito e ordinato il desktop del proprio computer.

## UTILIZZO DI SUPPORTI MAGNETICI

Gli utenti devono trattare con particolare cura i supporti magnetici (dischetti, nastri, DAT, chiavi USB, CD riscrivibili,…) in particolar modo quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati ivi contenuti. Di conseguenza le azioni da compiere obbligatoriamente sono le seguenti:
a) porre attenzione nell'utilizzo dei supporti rimovibili personali,
b) custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto (presso il custode delle password),

c) consegnare i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili, ...) obsoleti all'Amministratore di sistema per l'opportuna distruzione onde evitare che il loro contenuto possa essere successivamente alla cancellazione recuperato.

## PREVENZIONE DEI MALWARE

I virus sono programmi in grado di trasmettersi in modo autonomo e possono causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.
Oggi, meglio che soltanto di virus, è più corretto parlare di *malware*, che oltre ai virus comprendono - a titolo esemplificativo e non esaustivo - i cosiddetti *trojan* (cavalli di Troia), gli *Spyware* e altri strumenti e modalità di attacco difficilmente classificabili.
I mezzi a disposizione per difendersi dai *malware* includono la protezione dagli accessi non autorizzati, il ricorso esclusivo a fonti note e sicure per dati e programmi, l'uso dei software *antimalware* aggiornati.

L'Amministratore di Sistema, provvederà a:
- far installare e mantenere aggiornato un adeguato software *antimalware*;
- cancellare ogni *malware* intercettato e documentare ogni caso che si verifichi.

E' responsabilità dell'utente:
- Evitare di introdurre consciamente un *malware* nei computer.
- Utilizzare esclusivamente i supporti di memorizzazione (CD, DVD, USB, cassette, ecc.) ricevuti in dotazione.
- Non utilizzare programmi non autorizzati o software gratuito prelevato da siti Internet o in allegato a riviste o libri.
- Qualora si fosse costretti ad utilizzare supporti di memorizzazione (v. sopra) di incerta provenienza, effettuare prima una scansione *antimalware*.
- Ogni programma deve essere sottoposto alla scansione prima di essere installato.
- Non far partire, anche in modo accidentale, il computer da supporti esterni removibili (chiavette USB, CD, DVD…).
- Non utilizzare supporti già adoperati in precedenza o preformattati.
- Non utilizzare modem per la posta elettronica.
- Non scaricare da Internet, se non previa autorizzazione, file eseguibili o documenti da siti FTP.
- Non scaricare da Internet file di cui non si conosce o non si è ragionevolmente sicuri della fonte.
- Evitare di navigare in siti non consentiti o non affidabili (vedi anche più avanti l'apposito paragrafo "L'utilizzo di Internet")
- Non aprire e-mail di cui non si è certi della fonte, né i relativi allegati, in particolare se si dovesse trattare di file eseguibili (.exe) o compressi (.zip).
- Evitare di "cliccare" sui collegamenti (link) proposti all'interno delle e-mail.
- Contattare immediatamente l'Amministratore di Sistema qualora dovesse riscontrare o sospettare la presenza di *malware* nel computer che sta utilizzando.

## UTILIZZO DEI SERVER

I server di rete sono aree di condivisione di informazioni strettamente professionali 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, nemmeno per brevi periodi, in queste unità o sui PC locali.
L'Istituto si riserva la facoltà di procedere alla rimozione di ogni *file* o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente manuale.
Ogni utente è tenuto a memorizzare i propri file nella/e area/e del Sistema Informativo appositamente predisposte, e non dovrà memorizzare file nel "desktop" in quanto quest'ultimo non è sottoposto alle procedure di backup.
Particolare attenzione deve essere riposta nell'archiviare documenti a carattere riservato all'interno di cartelle situate sui server e condivisibili da più utenti del medesimo servizio o da parte di più uffici; è necessario infatti evitare che tali documenti possano essere letti o addirittura modificati da persone non autorizzate.
Sui Server vengono inoltre svolte le comuni e regolari attività di controllo, amministrazione e backup da parte del personale addetto.

# INTERNET E POSTA ELETTRONICA

## UTILIZZO DELLA RETE INFORMATICA

Le reti interne, presenti in ciascuno dei tre plessi (di scuola secondaria di primo grado e di scuola primaria), collegano tutti i computer presenti in ogni singolo edificio. L'accesso ad internet è gestito da quattro connessioni distinte: tre connessioni WDSL(CloudItalia), riservate alla segreteria, alle aule della scuola secondaria di primo grado (in via Peschiere, 16) e della scuola primaria (in via Fermi, 11) situate a Dosson di Casier e una connessione ADSL (Eolo)per la navigazione delle aule della scuola primaria di Casier (in via Basse, 1).
La rete informatica permette di salvare su server i files relativi alla produttività individuale.
Le cartelle presenti nei server di segreteria e di laboratorio sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back-up.
L'accesso è regolamentato da policies di sicurezza che suddividono gli accessi fra gruppi e utenti.
Periodicamente si provvede alla pulizia degli archivi, con cancellazione dei files obsoleti ed inutili.
Gli utenti della rete informatica sono tenuti a utilizzare la rete in modo conforme a quanto stabilitodal presente regolamento e quindi:
a) mantenere segrete e non comunicare a terzi, inclusi gli amministratori di sistema, le password d'ingresso alla rete ed ai programmi e non permettere ad alcuno di utilizzare il proprio accesso,
b) provvedere periodicamente alla pulizia degli archivi con cancellazione dei file obsoleti o inutili ed evitare un'archiviazione ridondante,
c) verificare preventivamente ogni archivio elettronico (file) acquisito attraverso qualsiasi supporto (es. pendrive) prima di trasferirlo su aree comuni della rete.

Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività della rete,interferendo con la connettività altrui o con il funzionamento del sistema e quindi di:
a) utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files o 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 delle privacy,
b) sostituirsi a qualcuno nell'uso dei sistemi, cercare di catturare password altrui o forzare password o comunicazioni criptate,
c) modificare le configurazioni impostate dall'amministratore di sistema,
d) limitare o negare l'accesso al sistema a utenti legittimi,
e) effettuare trasferimenti non autorizzati di informazioni (software, dati, ...),
f) distruggere o alterare dati altrui,
g) usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

## REGOLE PER LE PERSONE ESTERNE

Ai visitatori non è permesso connettere i propri equipaggiamenti direttamente alla rete dell'istituto.
Per l'accesso a Internet viene messa a disposizione degli ospiti una rete WiFi "Ospiti" separata a livello logico dalla rete d'Istituto.
Consulenti e altre persone esterne che operano con continuità possono essere inclusi nella rete interna con un ID personale e una password, previa autorizzazione del Dirigente Scolastico.

## UTILIZZO DELLE PASSWORD

Per l'accesso alla strumentazione informatica di Istituto ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione previste ed attribuite dall'incaricato della custodia delle password.
Le credenziali di autenticazione per l'accesso alla rete consistono in un codice per l'identificazione dell'utente (user id) associato ad una parola chiave (password) riservata che dovrà essere custodita dal Custode delle password con la massima diligenza e non può essere divulgata.

## PROCEDURE DI GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE

È necessario procedere alla modifica della parola chiave, a cura dell'incaricato, al primo utilizzo. Se l'utente non provvede autonomamente a variare la password entro i termini massimi, viene automaticamente disabilitato. Provvederà l'Amministratore di sistema a riabilitare l'utente e ad assegnargli una password provvisoria che l'utente dovrà cambiare al primo accesso.
Per scegliere una parola chiave si devono seguire le seguenti istruzioni:
-usare una parola chiave di almeno otto caratteri,
-usare una combinazione di caratteri alfabetici e numerici (meglio inserire anche segni di interpunzione o un carattere speciale),

-non usare mai il proprio nome o cognome, né quello di congiunti (le migliori passwordsono quelle facili da ricordare, ma allo stesso tempo difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe).
La password deve essere cambiata a intervalli regolari a cura dell'incaricato del trattamento d'intesa con il custode della password (minimo ogni sei mesi) e comunicata al custode delle password perché ne curi la conservazione.
Bisogna evitare di comunicarla ad altri, di trascriverla su supporti (agenda, post-it, ...) che siano accessibili ad altri o di consentire che qualcuno sbirci quello che si sta scrivendo sulla tastiera quando viene immessa la password.
Nel caso si sospetti che la password abbia perso la segretezza essa deve essere immediatamente sostituita.

## UTILIZZO DI INTERNET

Il sistema informativo ed i dati in esso contenuti possono subire gravi danneggiamenti per un utilizzo improprio della connessione alla rete internet; inoltre, attraverso la rete possono essere introdotti nel sistema virus informatici Spyware, Malware, e possono attraverso "backdoor" penetrare utenti non autorizzati.

Internet è da considerarsi uno strumento lavorativo e pertanto l'utilizzo di Internet da parte dei dipendenti dovrà essere adeguato a scopi e obiettivi scolastici e conforme agli standard di comportamento dell'Istituto.

L'accesso ad internet è regolato da filtri predefiniti dall'amministratore di sistema su autorizzazione dell'amministrazione, con esclusione dei siti istituzionali.
Il Titolare del trattamento provvede alla individuazione delle categorie di siti considerati correlati o non correlati con la prestazione lavorativa.
L'Amministratore di sistema provvede alla configurazione di sistemi e all'utilizzo di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software).
L'accesso alla navigazione in internet deve essere effettuato esclusivamente a mezzo della rete di istituto e solo per fini lavorativi o di studio. L'utilizzo responsabile di modem personali è sconsigliato e comunque deve essere autorizzato dall'Amministratore di sistema.
Gli utenti sono tenuti ad utilizzare l'accesso ad internet in modo conforme a quanto stabilito dal presente regolamento e quindi devono navigare solamente in siti attinenti allo svolgimento delle mansioni assegnate.
Agli utenti è fatto espresso divieto di qualsiasi uso di internet che possa in qualche modo recare danno all'istituto o a terzi e quindi di:
a) fare conoscere ad altri la password del proprio accesso,
b) usare internet per motivi personali,
c) servirsi dell'accesso internet per attività in violazione del diritto d'autore o di altri diritti tutelati dalla normativa vigente,
d) utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Winmx, e-Donkey,…)
g) ascoltare la radio o guardare video o filmati utilizzando le risorse internet, se non attinenti l'attività lavorativa o direttamente autorizzati dal responsabile del trattamento,
h) effettuare transazioni finanziarie, operazioni di remote banking, acquisti on-line e simili, se non attinenti l'attività lavorativa o direttamente autorizzati dal Responsabile del trattamento,
i) inviare fotografie, dati personali o di amici dalle postazioni internet.
Al termine dell'utilizzo della rete è obbligatorio effettuare il logout.

## UTILIZZO DELLA POSTA ELETTRONICA

L'Istituto mette a disposizione dei lavoratori indirizzi di posta elettronica individuali in dominio istituzionale @iccasier.it (servizio di posta interno all'Istituto) che consentono:

- di inviare e ricevere comunicazioni attinenti allo svolgimento dell'attività lavorativa,
- di partecipare a gruppi di lavoro in condivisione e collaborazione, attinenti allo svolgimento dell'attività lavorativa.

Tramite la posta istituzionale con dominio @iccasier.it possono essere trasmesse le seguenti comunicazioni:
- convocazioni riunioni;
- comunicazioni di servizio anche dirette al singolo dipendente;
- materiale preparatorio alle riunioni collegiali;
- circolari;
- copia elettronica di documenti redatti su supporti cartacei (purché in formati e dimensioni opportune).

Ogni utente assegnatario di una casella di posta elettronica istituzionale è responsabile del corretto utilizzo della stessa ed è tenuto a utilizzarla in modo conforme a quanto stabilito dal presente regolamento, quindi deve:
a) conservare la password nella massima riservatezza e con la massima diligenza,
b) mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti,
c) utilizzare l'account per l'invio di comunicazioni attinenti all'attività lavorativa,
d) inviare preferibilmente file in formato PDF,
e) al termine delle operazioni effettuare il logout dall'account.

Agli utenti è fatto divieto di qualsiasi uso della posta elettronica che possa in qualche modo recare danno all'istituto o a terzi e quindi di:
a) prendere visione della posta altrui,
b) simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza,
c) utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'istituto,
d) trasmettere a mezzo posta elettronica dati sensibili, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati,
e) utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni, messaggi tipo "catene" e altre e-mails che non siano di lavoro.

## UTILIZZO DELLE LIM

Le LIM in dotazione alle aule devono essere correttamente utilizzate. Ogni danno, non provocato dalla normale usura, ma imputabile ad atti vandalici, a incuria o a un utilizzo non appropriato dell'attrezzatura, sarà addebitato al responsabile del guasto o, qualora non fosse possibile individuarlo, a tutta la classe (vedi Regolamento d'Istituto).

I Docenti sono tenuti a :

- spegnere il videoproiettore quando non è in uso;
- non spegnere mai l'interruttore della presa o della ciabatta;

- non far cadere le penne interattive;
- non staccare cavi USB, cavi elettrici, alimentatori, cavi di rete;
- non aggiungere alcun device diverso dalla normale dotazione d'aula;
- non scrivere con pennarelli normali sulle LIM;
- non lasciare incustodita l'aula senza aver preventivamente chiuso a chiave la porta.

Gli Studenti sono tenuti a:

- non spegnere mai l'interruttore della presa o della ciabatta;
- non far cadere le penne interattive;
- non urtare con violenza le superfici interattive;
- non scrivere con pennarelli normali sulle LIM;
- non staccare cavi USB, cavi elettrici, alimentatori, cavi di rete.

## UTILIZZO DELLE STAMPANTI

Stampanti e materiali di consumo in genere (carta, inchiostro, toner, supporti digitali come CD e DVD) possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi e utilizzi eccessivi.
Gli utenti devono effettuare la stampa dei dati solo se strettamente necessaria e ritirare prontamente dai vassoi delle stampanti comuni i fogli per impedire a persone non autorizzate di accedere alle stampe di documenti riservati, distruggere personalmente e sistematicamente le stampe che non servono più.
La stampante 3D è ad esclusivo utilizzo delle docenti appositamente formate. È severamente vietato avvicinarsi e toccarla soprattutto quando è in funzionamento.

## UTILIZZO DI TELEFONI E ALTRE APPARECCHIATURE

Il telefono affidato al dipendente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa.
La ricezione o l'effettuazione di telefonate personali sono consentite solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso a disposizione.
Al cellulare d'Istituto qualora venisse assegnato, si applicano le medesime regole sopra previste.

È vietato l'utilizzo del fax e delle fotocopiatrici d'Istituto per fini personali.
È fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi, salvo:
a) diversa disposizione esplicita del titolare del trattamento, da concordarsi di volta in volta e comunque sempre preventivamente al trattamento,
b) informazione preventiva degli interessati,
c) acquisizione del loro libero consenso, preventivo ed informato.

## GESTIONE DEL SITO WEB DELLA SCUOLA

L'Istituzione Scolastica possiede un Sito Web per la gestione del quale è stato nominato un referente.
In nessun caso l'Istituto Comprensivo potrà essere ritenuto responsabile dei danni di qualsiasi natura causati direttamente o indirettamente dall'accesso al sito, dall'incapacità o impossibilità di accedervi, dall'affidamento dell'utente e dall'utilizzo dei contenuti.
L'Istituto provvederà ad inserire nel sito informazioni e comunicazioni aggiornate, rubriche, notizie, eventi, articoli relativi alle attività didattiche dell'Istituto.
I documenti sono pubblicati in formato .pdf.
Le informazioni relative alle persone da contattare includono solo l'indirizzo (posta elettronica e numero telefonico) della scuola e non dati personali.

## GESTIONE ED UTILIZZO DEL REGISTRO ELETTRONICO

L'Istituzione Scolastica possiede un registro elettronico gestito da un Amministratore.
Tutti i dati relativi agli utenti che utilizzano il software sono protetti da password e sarà compito di ogni utente conservare e custodire le proprie credenziali. Ogni docente è tenuto a procedere con il log out al termine della lezione e comunque ogni volta in cui si debba allontanare dalla postazione.

## ACCESSO AI DATI SUL SISTEMA INFORMATIVO IN CASO DI ASSENZA O DI CESSAZIONE DEL RAPPORTO DI LAVORO

Qualora si rendesse necessario, per impedimento o prolungata assenza di un incaricato, accedere ai dati da questi trattati e non fosse possibile farlo attraverso un utente con profilo/ruolo ed incarico analogo, il Dirigente ha la facoltà di richiedere all'Amministratore di Sistema di disabilitare la password dell'incaricato assente ed inserirne una provvisoria di durata temporanea.
A tal fine il Dirigente invierà una e-mail di richiesta all'Amministratore di Sistema al fine di resettare le credenziali del dipendente assente.
Il Dirigente provvederà poi a darne debita informazione all'incaricato al suo ritorno, affinché questi possa ripristinare al più presto la segretezza delle proprie credenziali.
Si ritiene comunque opportuno, ogni qualvolta possibile, contattare preventivamente l'incaricato assente e concordare con quest'ultimo le modalità di gestione della specifica esigenza (ad esempio designando e autorizzando un collega ad accedere ai dati previo reset della password e inserimento di password temporanea).
Alla cessazione del rapporto di lavoro di un dipendente abilitato ad accedere al Sistema Informativo, il Dirigente informerà l'Amministratore di Sistema che provvederà immediatamente, a far disattivare le utenze (account di rete, casella email, user gestionale); la cancellazione effettiva dei dati dell'utente sarà effettuata al più presto a meno che non ne richieda esplicitamente il mantenimento specificandone finalità e durata (via email all'Amministratore di Sistema, in copia al Dirigente) e comunque per un massimo di 30 giorni.
L'Amministratore di Sistema su indicazione del Dirigente dovrà assicurarsi che l'utente – prima della cessazione – provveda a rendere disponibili i propri dati, file e messaggi e-mail,

memorizzati nel Sistema Informativo e a concordare per tempo tempistica e modalità di disattivazione dell'account di rete, casella email e utenza software gestionale.

# DIRITTI E RESPONSABILITÀ DEI DIPENDENTI

Per assicurare la tutela dei diritti, delle libertà fondamentali e della dignità dei lavoratori, garantendo che sia assicurata una ragionevole protezione delle loro sfera di riservatezza nelle relazioni personali professionali, il trattamento dei dati mediante l'uso delle tecnologie telematiche è conformato al rispetto dei diritti delle libertà fondamentali nonché della dignità dell'interessato, dei divieti posti dallo statuto dei lavoratori sul controllo a distanza e dei principi di necessità, correttezza e finalità determinate, esplicite e legittime.
Ogni utente è responsabile, sia sotto il profilo civile che penale, del corretto uso delle risorse informatiche, dei servizi e dei programmi ai quali ha accesso e dei dati che tratta.
Spetta ai docenti vigilare affinché gli studenti loro affidati rispettino il regolamento e sono ne direttamente responsabili.

# CONTROLLI E SANZIONI

Il datore di lavoro, per esigenze organizzative, per garantire la sicurezza sul lavoro, per evitare reiterati comportamenti dolosi illeciti può avvalersi legittimamente, nel rispetto dell'art. 4 comma 2 dello Statuto dei lavoratori, di sistemi che consentano un controllo a distanza e determinato di dati personali riferibili a singoli utenti.
La lettura e la registrazione sistematica del servizio di accesso ad internet vengono automaticamente registrate.
Tali file possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazionedella normativa vigente.
Le registrazioni possono essere utilizzate per fornire informazioni esclusivamente su:
-numero di siti visitati da ciascun utente, quantità totale di dati scaricati, postazioni di lavoro utilizzate per la navigazione.
Qualora i controlli evidenzino un utilizzo anomalo degli strumenti informatici dell'istituto, il titolare del trattamento procede in forma graduata:
-in via preliminare si eseguono controlli su dati aggregati, in forma anonima e si provvede ad un avviso generalizzato agli utenti,
-se perdurano le anomalie si procede a controlli per tipologie di locali di utilizzo (uffici, aule, ...) o tipologie di utenti (ata, docenti, studenti, ...) e si procede con avvisi mirati alle categorie di utilizzatori,
-ripetendosi l'anomalia, sarà lecito il controllo su base individuale e si procederà all'invio di avvisi individuali,
-in caso di verificato e reiterato uso non conforme delle risorse informatiche il titolare del trattamento attiva il procedimento disciplinare nelle forme e con le modalità previste dall'Istituto per gli studenti (vedere Regolamento di Istituto e di disciplina), dai contratti di lavoro per i dipendenti e attraverso l'adozione degli atti di specifica competenza nel caso di personale non dipendente,
-può portare alle azioni civili e penali consentite.

L'utilizzo dei servizi di accesso ad internet cessa o viene sospeso d'ufficio quando:
-non sussiste più la condizione di dipendente/studente o l'autorizzazione al loro uso,
-vi è il sospetto di manomissione dell'hardware o del software,
-in caso di diffusione o comunicazione a terzi da parte del dipendente di password, codici di accesso ecc. ...,
-in caso di accesso doloso a file o servizi non rientranti tra quelli autorizzati,
-ogni qualvolta sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente che mette a rischio il sistema.

## INFORMATIVA AGLI UTENTI

Il presente regolamento è messo a disposizione degli utenti, per la consultazione, sui mezzi di comunicazione interna utilizzati dall'istituto (circolare, registro elettronico, sito) e quindi portato a conoscenza di ciascun utente.
Qualora l'Istituto decidesse di perseguire, per fini legati alla sicurezza dell'intero sistema informativo, il controllo della posta elettronica e della navigazione in internet, quest'ultimo viene informato degli strumenti e dei modi di trattamento effettuati prima che questo inizi.

## AGGIORNAMENTO E REVISIONE DEL REGOLAMENTO

Il presente regolamento è soggetto a revisione con frequenza annuale e ogni qualvolta sia necessario un aggiornamento alla luce dell'esperienza, di nuove normative e dell'innovazione tecnologica.
Tutti gli utenti possono proporre quando ritenuto necessario, integrazioni al presente regolamento e le proposte saranno esaminate dal Responsabile del trattamento in collaborazione con l'Amministratore di sistema.

Il Dirigente Scolastico
Nicola Labate